094956/EU XXVIII. GP
Eingelangt am 02/10/26

Council of the
European Union

Brussels, 2 October 2026
(OR. en)

13928/26
ADD 2

Interinstitutional Files:
2026/0301 (COD)
2026/0308 (COD)

JAI 1239
SCHENGEN 29
ENFOPOL 359
ENFOCUSTOM 115
CYBER 397
CODEC 1828
CADREFIN 417
IA 254
PROCIV 190
TELECOM 464

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	1 October 2026
To:	Ms Thérèse BLANCHET, Secretary-General of the Council of the European Union
No. Cion doc.:	SWD(2026) 1010 final
Subject:	COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT REPORT Accompanying the documents Proposal for a Regulation of the European Parliament and of the Council on establishing the European Criitcal Communication System Proposal for a Regulation of the European Parliament and of the Council establishing the framework for the use of the European Critical Communication Sysrem by the Member States' services and other organisations in charge of civil protection

Delegations will find attached document SWD(2026) 1010 final.

Encl.: SWD(2026) 1010 final

www.parlament.gv.at

EUROPEAN
COMMISSION

Brussels, 30.9.2026
SWD(2026) 1010 final

COMMISSION STAFF WORKING DOCUMENT

IMPACT ASSESSMENT REPORT

Accompanying the documents

Proposal for a Regulation of the European Parliament and of the Council on establishing the European Criitcal Communication System

Proposal for a Regulation of the European Parliament and of the Council establishing the framework for the use of the European Critical Communication Sysrem by the Member States' services and other organisations in charge of civil protection

{COM(2026) 1010 final} - {SEC(2026) 1010 final} - {SWD(2026) 1011 final}

www.parlament.gv.at

Table of contents

GLOSSARY 2
1. INTRODUCTION: POLITICAL, LEGAL AND TECHNOLOGICAL CONTEXT 3
2. PROBLEM DEFINITION 6
3. WHY SHOULD THE EU ACT? 16
4. OBJECTIVES: WHAT IS TO BE ACHIEVED? 18
5. WHAT ARE THE AVAILABLE POLICY OPTIONS? 21
6. WHAT ARE THE IMPACTS OF THE POLICY OPTIONS? 32
7. HOW DO THE OPTIONS COMPARE? 39
8. PREFERRED OPTION 45
9. HOW WILL ACTUAL IMPACTS BE MONITORED AND EVALUATED? 46
ANNEX 1: PROCEDURAL INFORMATION 48
1. LEAD DG, DECIDE PLANNING/CWP REFERENCES 48
2. ORGANISATION AND TIMING 48
3. CONSULTATION OF THE RSB 49
4. EVIDENCE, SOURCES AND QUALITY 49
ANNEX 2: STAKEHOLDER CONSULTATION (SYNOPSIS REPORT) 51
ANNEX 3: WHO IS AFFECTED AND HOW? 56
1. PRACTICAL IMPLICATIONS OF THE INITIATIVE 56
2. SUMMARY OF COSTS AND BENEFITS 56
3. RELEVANT SUSTAINABLE DEVELOPMENT GOALS 57
ANNEX 4: ANALYTICAL METHODS 59
ANNEX 5: COMPETITIVENESS CHECK 64
ANNEX 6: SME CHECK 67
ANNEX 7: ADDITIONAL MATERIALS 71

www.parlament.gv.at

GLOSSARY

3GPP	3rd Generation Partnership Project. A global collaboration project that develops and maintains standards for mobile telecommunications, including 3G, 4G, 5G, and Internet of Things technologies.
Broadband	The transmission of data over a wide range of frequencies, allowing for high-speed and simultaneous transfer of multiple data streams. Used for example for video and other large data.
LTE	Long-Term Evolution is a wireless broadband communication standard designed to provide high-speed mobile data and improved network efficiency, forming the foundation of modern 4G networks.
MCX	Mission-Critical Services is a standardized suite of communication services designed to ensure reliable, secure, and low-latency communications for public safety and other critical operations.
MNO	Mobile Network Operator.
Narrowband	A method of transmitting data over a small frequency range, optimized for long-distance, low-data-rate, and energy-efficient communication. Typically used for voice communication.
Quality, Priority and Pre-emption (QPP)	A framework used in telecommunications to manage network resources effectively. It enables networks to prioritize mission-critical services, ensuring that essential applications get the necessary resources.
TETRA/ Tetrapol	A digital professional mobile radio standard used for secure voice and data communication, primarily by emergency services and military organisations worldwide.
Testbeds	A collection of technical equipment and software where different configurations and operational situations are trialled.

www.parlament.gv.at

1. INTRODUCTION: POLITICAL, LEGAL AND TECHNOLOGICAL CONTEXT

This Impact Assessment Report accompanies the legislative proposal to establish the **European Critical Communication System (EUCCS)**, interconnecting EU Member States and Schengen Associated Countries' (hereinafter referred to as "Member States") next-generation mission-critical communication systems**.**

EUCCS will serve more than 5 million first responders in emergency services[1] across Europe in their daily life-saving operations and during major emergencies. Emergency services typically include law enforcement, rescue and health/medical services, and firefighters. They may, depending on the situation, also include other public entities in charge of security and safety. Their effective response requires that emergency services can communicate with each other, whenever and wherever they are.

For this document, **critical communication systems** refer to mobile radio communication systems and devices used by emergency services[2] with specific requirements in terms of reliability, security and availability. These systems are built to withstand disruption and continue to operate even when other communication channels fail. They are crucial for coordinating the response to emergency and crises and thus ultimately help saving lives. It is important to distinguish critical communication the various ongoing initiatives to improve **secure communications**. While there are overlaps in terms of technology and user groups, secure communication does not serve mission critical needs and is not designed for emergency response.

Evidence basis for the Impact Assessment

This Impact Assessment Report is based on multiple sources, notably a study by an independent consortium, targeted interviews with Member States, industry, and the contribution of the *Commission Expert Group with Member States on Mission Critical Communication* (hereinafter referred to as '*mission-critical communication group*'). HOME published also a *Call for Evidence and a Commission Open Public Consultation*[3]. The Impact Assessment Report also builds on the *EUCCS Operational Plan*, a roadmap for establishing the system of systems adopted by the mission critical communication group in May 2025. Finally, it builds on the results stemming from EU-funded security research activities, involving Member States and European industry, and continuously validated in dedicated trials by more than 600 responders from emergency services from

[1] That figure is based on the number of expected users of EUCCS, as communicated by Member States. this is not the number of interventions, but of *personnel* that uses critical communication means, and thus will benefit directly from EUCCS. The number is based on a questionnaire to Member States' competent authorities in which they were asked for report the expected number of users (such as police officers, firefighters, medical services) to DG HOME.

[2] 'Emergency service' means a service, recognised as such by the Member State, that provides immediate and rapid assistance in situations where there is, in particular, a direct risk to life or limb, to individual or public health or safety, to private or public property, or to the environment, in accordance with national law. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32018L1972.

[3] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14532-European-Critical-Communication-System/public-consultation_en.

www.parlament.gv.at

20 Member States. The technological solutions were developed in almost 10 years of EU-funded projects *BroadMap*[4], *BroadWay*[5], and *EUCCS Preparation*[6].

Political context

EUCCS is based on a strong political mandate. Technical and operational coordination projects leading later to EUCCS were enhanced as response to the 2015-2016 wave of terrorist attacks, which highlighted the lack of communication among emergency services in major crisis situations. The initiate thus follows long-term and strategic approach that is based on concrete operational needs. A key milestone was the *Council Conclusions of 7 June 2021 on the protection of public spaces*, which emphasised the importance of secure, interoperable mission-critical communication. The Covid-19 Pandemic as well as the Russian war of aggression against Ukraine further highlighted the importance of improved critical communication capabilities, across different sectors. The *EU Space Strategy for Security and Defence* mentioned for the first time the creation of a European Critical Communication System as goal for the Commission.[7] In 2023, the European Commission established thus the expert group on mission-critical communication to support it in the establishment of EUCCS.

The political commitment was reiterated in 2024 in the *Commission White Paper 'How to master Europe's digital infrastructure needs'*, which announced to establish EUCCS by 2030.[8] Further momentum came with the *2024–2029 Political Guidelines* of Commission President von der Leyen, which stated that *"our united approach to security should be centred around a new European Critical Communication System (...)".* Also, the Niinistö Report[9] urged the EU to complete the EUCCS as soon as possible and recommended to ensure its interoperability with systems used by armed forces. This direction was reaffirmed in 2025 in *ProtectEU – the European Internal Security Strategy*[10] and the *European Preparedness Union Strategy*, both announcing a legislative initiative[11] Consequently, the legislative proposal establishing EUCCS has been included in the Commission's Work Programme for 2026.

Legal context

There are existing and proposed legal acts in the EU that cover areas that are relevant for critical communication, notably acts establishing operational cooperation in civil protection including emergency response, acts regulating the resilience of communication networks (such as the NIS-2 Directive), and acts that regulate the telecommunication sector, including rules for public safety (such

---

[4] Horizon 2020 project (2016-2017). The primary goal was to collect and validate the operational requirements of emergency services with the aim to establish a core set of specifications, and a roadmap for interoperable radio communication solutions. https://cordis.europa.eu/project/id/700380.

[5] Horizon 2020 project (2018-2023). Using pre-commercial procurement, emergency services from eleven Member States and European companies developed and demonstrated in this project technological solutions for a pan-European interoperable broadband mobile system. https://cordis.europa.eu/project/id/786912.

[6] The on-going project funded from the Internal Security Fund started in 2022. https://euccs.eu/ The demand for building EUCCS is most importantly formulated by the EUCCS Preparation Projects and its precursors. In this framework, emergency service personnel themselves formulate and substantiate the need. This is furthermore substantiated by the results of the Open Public Consultation. A summary of all consultation activities, that relied primarily on evidence from Member States and their emergency services, can be found in Annex 4.

[7] https://defence-industry-space.ec.europa.eu/eu-space/eu-space-strategy-security-and-defence_en.

[8] European Commission, *White Paper: How to Master Europe's Digital Infrastructure Needs* (2024) https://digital-strategy.ec.europa.eu/en/library/white-paper-how-master-europes-digital-infrastructure-needs.

[9] Niinistö, S. (2024), *Safer Together – Strengthening Europe's Civilian and Military Preparedness and Readiness*, p. 59 and p. 69.

[10] COM (2025)148final (2025) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025DC0148.

[11] European Commission (2025), *European Preparedness Union Strategy*, JOIN(2025) 130 final.

www.parlament.gv.at

as the '112' and eCall provisions) as part of the Electronic Communications Code and the proposed Digital Networks Act. Still, there is no existing legal framework on which EUCCS could be based. In fact, the call for the Commission to put forward a proposal for legislation to establish EUCCS came from Member States acknowledging that a system of such scope and size can only be realised with an appropriate regulatory framework.

Armed forces in Europe are another major user group of critical communication. In some Member States, they can share some of the critical communication networks used by civil emergency services, while in other Member States there is a separation due to technical, operational or legal reasons. At EU-level, there is only a legal basis to regulate critical communication for civil emergency responders (see 3.1) therefore this initiative is addressing civil emergency services. There are however various non-legislative activities taken by the Commission to respond the recommendation of the Niinistö report and ensure interoperability of EUCCS with systems used by armed forces in Europe, which will also ensure its contribution in countering hybrid threats.[12]

Technological context

The U.S. system 'FirstNet' is a key reference point and has been studied by DG HOME intensively, including during site visits in the United States. While on the technological and end-user side (a broadband system for all types of emergency services) there are important similarities, there exist also key differences: FirstNet is provided by one single Mobile Network Operator (AT&T) across the whole territory of the U.S. For that, dedicated spectrum is available that is allocated to emergency services. Thus, the model cannot be replicated in the EU, given there are neither EU-wide Mobile Network Operators, nor is it possible to simply harmonise or reserve spectrum via the EUCCS Regulation. On international provisions that may affect digital sovereignty, it is important to underline that the proposed EUCCS Regulation will only very partially be able to address those matters. The question of digital sovereignty in relation to the U.S. is a much wider policy are and concerns telecommunication and digital policy. However, EUCCS will spell out minimum resilience requirements, which include Member States' control over the critical parts of the network. This builds on existing practices in Member States and is in line with the overall cybersecurity and 5G/6G policy of the Union. EUCCS and Member States' next generation critical communication systems will adhere to the globally defined 3GPP (3rd Generation Partnership Project) standards, which have a specific working group on mission critical communication. Since broadband communication of emergency services will run over commercial networks, the alignment to the 3GPP mobile standards is a must. To ensure additional resilience and security, an additional

Sustainable Development Goals (SDGs)

By enabling critical cross-border communication, EUCCS strengthens the capacity of emergency services and supports efficient coordination in emergency and crisis situations, accelerates response to disasters and emergencies, and enhances accountability and reliability. The general and specific objectives of the EUCCS contribute to various UN SDGs[13], notably: SDG no. 11 - Make cities and human settlements inclusive, safe, resilient and sustainable; SDG no. 13 - Strengthen resilience and adaptive capacity to climate-related hazards and natural disasters in all countries; and SDG no. 16 - Promote peaceful and inclusive societies for sustainable development, provide access to justice for all and build effective, accountable and inclusive institutions at all levels

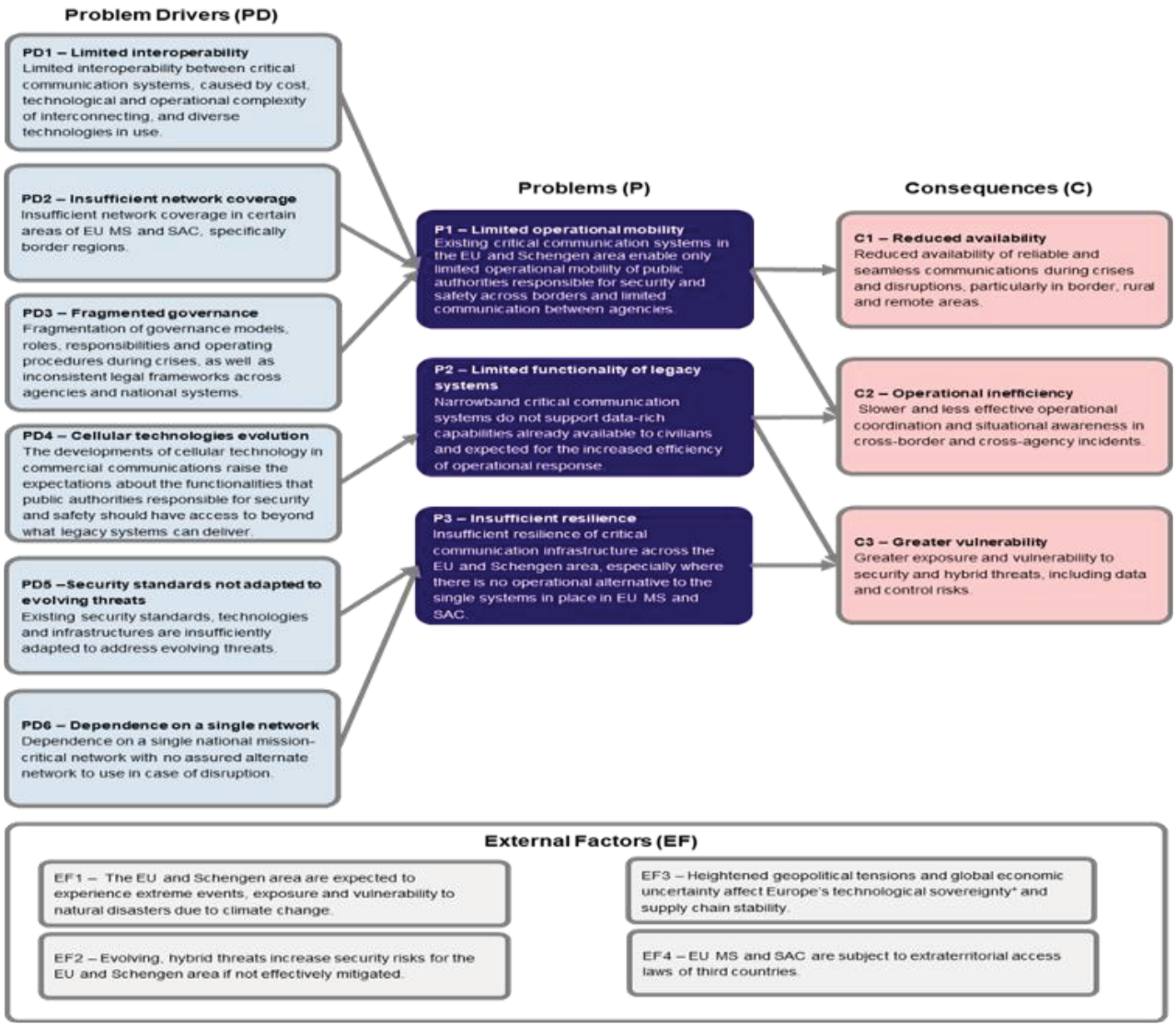
[12] The Mission Critical Communication Group has a working team on dual-use and regular work is being conducted with European Defence Agency, the EU Military Staff and NATO.
[13] https://sdgs.un.org/goals.

www.parlament.gv.at

2. PROBLEM DEFINITION

Based on comprehensive stakeholder consultations, ten years of technical preparation projects, and exchanges with Member States, emergency services and industry, **three main problems** have been identified that the planned EU legislation needs to address. The problems, underlying problem drivers and consequences are presented below.

Figure 1: Problem Tree



2.1. What are the problems (Ps)?

P1 - Existing critical communication systems enable only limited operational mobility of public authorities responsible for security and safety across borders and limited communication between emergency services.

Critical communication systems in the EU and Schengen area are operated in isolation, with very limited interconnection across borders and between emergency services within Member States. In Europe there are two main mission critical communication systems, namely TETRA and Tetrapol whose initial development date back decades, when interoperability requirements and cross-border

www.parlament.gv.at

cooperation were much less a priority[14]. Equipment from TETRA and Tetrapol can therefore neither be operated in the other technology's network, nor in networks from different vendors. That is caused by the fact that different technical standards were used (TETRA and Tetrapol, see further below), as well as the absence of a European framework to harmonise their deployment and evolution. This means that to this day communication between different emergency services is complicated and whenever responders cross a border, their communication equipment cannot be used. This leads to significant problems in daily operations, as well when responding to major emergencies[15]. 13 out of 25 Member States still operate narrowband-only systems (TETRA/Tetrapol), while 12 Member States report hybrid configurations combining narrowband with some form of broadband (trials).

Interviews with EU institutions and agencies, Member States' authorities, and emergency services confirmed that cross-border joint operations are hindered by the absence of interconnection between critical communication systems. For all types of emergency services, evidence shows a however a clear need for communication in cross-border or near-border incidents[16], with an increase in cross-border incidents over the past five years[17]. It is however not possible to give a definitive number on all cross-border operations of all emergency services in Europe, as this number is neither collected anywhere, nor would it be comparable.

The operational need is shown for example by the number of joint operations at the Schengen borders[18], as well as in context of the EU-funded project EU-Patrols[19]. Between 2022 and 2025, nearly 1,000 joint patrol missions have been carried out to fight crime. Information comes from questions asked to Member States' emergency services on how much incidents have a cross-border or near-border nature, in which 19 Member States (out of 25) estimated this number to reach 10%. A significant number of Member States furthermore report an increase of such incidents. Additionally, in the European Multidisciplinary Platform Against Criminal Threats (EMPACT) Framework[20] over 300 operational actions take place annually. Finally, 50 joint centres currently exist across the Schengen Area and 59 in Europe. These centres are set up between two or more Member States. Another indicator is the number of prepositioned firefighters across Member States. This number is expected to reach 770 this year.

Forest fires and any other deployments of the UCPM are a key use-case for EUCCS. EUCCS covers all communication means of emergency services, be they ground-based, waterborne or aerial. A table detailing the increase of EUCPM activations is included in Annex 7[21].

Figure 2: Map showing prepositioned Ground Forest Firefighting teams deployed through the UCPM in 2025

---

[14] TETRA, or Terrestrial Trunked Radio is a global standard for digital radio technology. In contrast, Tetrapol is a 1988 proprietary technology even if its specification is publicly available.

[15] Informal Commission Expert Group on Mission Critical Communication (MCCG), *Opinion 1/2025: Plan for Developing the European Critical Communications System (EUCCS)*, Version 1.0 (8 May 2025).

[16] Based on answers to the survey question "In your experience, what percentage of public security and safety incidents require cross-border communication?": 19 out of 25 respondents estimated that up to 10% of incidents require cross-border communication.

[17] Based on the survey question "Have you observed an increase in the number of cross-border incidents over the past five years?": 11 out of 25 report a slight or significant increase.

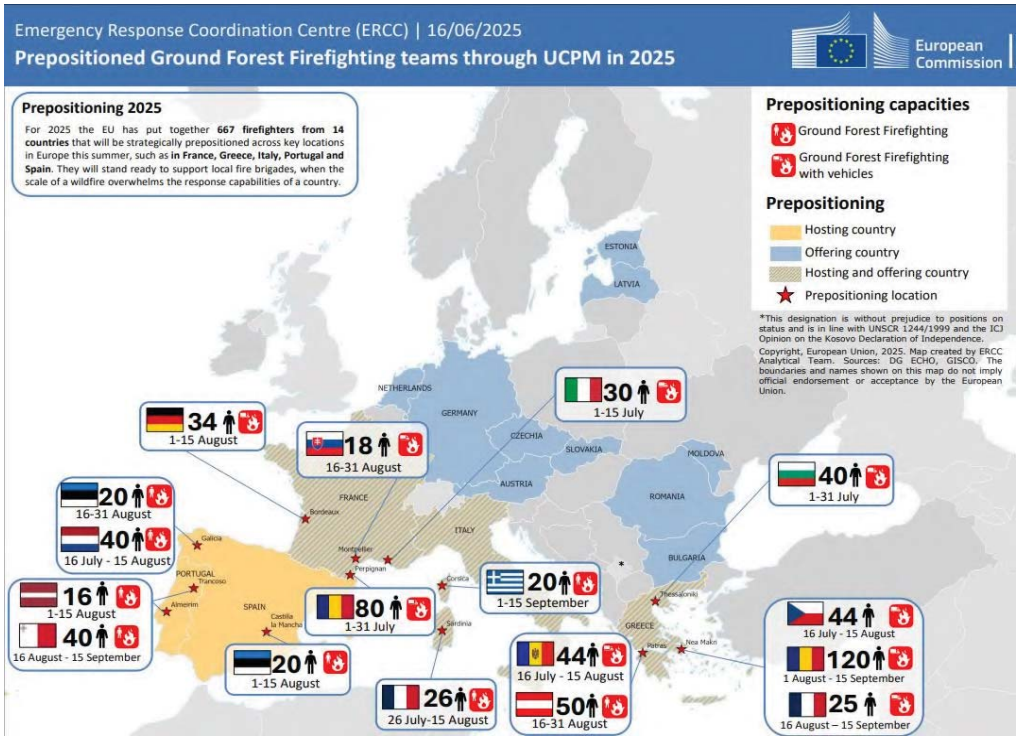
[18] In 2025 State of Schengen Report, it is highlighted that cross-border cooperation, particularly at the regional and border areas, has improved significantly over the past year.

[19] Protecting together: EU funded project EU-Patrols in action

[20] EMPACT – fighting crime together

[21] See Annex 7, figure 1.

www.parlament.gv.at



Thus, the growing operational need for cross-border communication and communication between emergency services is not reflected by existing systems: in the survey[22], 19 out of 25 Member States stated that the current critical communication systems do not sufficiently support interoperability with other Member States. Furthermore, 16 out of 25 Member States reported that handover and roaming is a problem in their cross-border critical communications[23]. There have been previous attempts at connecting TETRA systems, but only the Nordic countries - Norway, Sweden and Finland - succeeded in integrating their networks in the Inter-System Interface (ISI)[24]. Attempts to replicate the Nordic success at EU-level did not yield tangible results[25].

For instance, the EU-funded project *Inter System Interoperability for TETRA-TetraPol Networks (ISITEP)*, developed a cross-border communication infrastructure based on IP integration[26]. It was not further pursued for logistical, budgetary and operational reasons (see chapter *2.1.2. Limited functionality of legacy systems).*

While the lack of inter-operability has always been a problem, the pressure to solve it is now much higher than it was in the last decades as the operational and legal reality has evolved and cross-border and EU-wide missions for all types of emergencies are much more frequent than they were. A detailed

[22] Throughout the study, the term survey refers to the surveys conducted in the framework of the independent study. The visualisation of their results is included in Annex 7. While the study (which was of high quality) is a key element of the report, the Commission nevertheless conducted its own assessment thoroughly. Stemming from that, there is the difference in the preferred option, where the study favoured PO 2.2 (system of systems with centralised governance), while the Commission identifies PO 2.1 (system of systems decentralised governance).
[23] See Annex 7, figures 1 and 2.
[24] Norway and Sweden Interconnect Secure Radio Communication Networks - TCCA.
[25] However, many of the key lessons have been translated into EUCCS via the EUCCS Preparation Project, which included since its start experts from ISI. Notably the need to supplement technical interoperability with Operational Procedures and to set up a governance for the system to function are lessons-learnt from the Nordics. The same is true for the experience of international partners, notably the U.S. FirstNet.
[26] Inter System Interoperability for Tetra-TetraPol Networks | FP7 | CORDIS | European Commission.

www.parlament.gv.at

breakdown of the maturity level of national critical communication systems is available in Annex 7[27].

P2 – Narrowband critical communication systems do not support data-rich capabilities available to civilians and required for increased efficiency of operational response.

Emergency response is increasingly dependent on the rapid exchange of digital information such as incident imagery, video, live location and structured data. Like it is already common for commercial telecommunication, emergency services need to shift coherently from the narrowband technologies to broadband, which allows transmission of data over a wide range of frequencies, facilitating for high-speed and simultaneous transfer of multiple data streams. Yet, emergency services in Member States still depend on narrowband critical communication systems such as TETRA or Tetrapol, which provide only limited data capacity as they were initially designed for voice and short messaging. This creates efficiency losses, because information that is available early in an incident cannot be shared securely and systematically over the mission-critical network, leading to delays and incomplete situational awareness. Stakeholders describe this as a practical constraint that limits their efficiency. They highlight the increasing need to transfer voice, pictures and video data for improved operational coordination and situational awareness[28].

P3 – Insufficient resilience of critical communication infrastructure across the EU and Schengen area

Critical communication infrastructure is a prime target for malign actors, including both State and non-State actors. Threats range from cyber-attacks, jamming, and electromagnetic interference to physical sabotage. At the same time, critical communication systems can be disrupted by the impact of natural disasters, such as floods and fires as well as by network problems, caused namely by overload. According to Member States' authorities, the threat landscape affecting critical communication systems has evolved significantly over the past decade, with the frequency and impact of incidents accelerating. Therefore, comprehensive resilience including back-up, re-routing and redundancy is essential to ensure the functioning of critical communication systems.

There are several concrete examples of the failure of critical communication systems, including the 2016 Brussels terrorist attacks, in which also the commercial mobile networks failed due to overload; the floods of summer 2022 affecting notably Germany and Belgium in which communication base stations were destroyed; as well as the 2025 blackout in Spain and Portugal in which lack of power led to disruption of networks. The examples confirm the collected data at European level via the survey across Member States, which show that a number of Member States identified problems with the resilience of critical communication systems[29].

---

[27] Annex 7, figures 2 and 3.

[28] Feedback from the EUCCS Preparation trials carried out in Italy (November 2025) and Germany (March 2026).

[29] See Annex 7, figure 5. Critical communication systems must have very high reliability, since their disruption has direct impact on the ability to respond to emergencies. Thus, the fact that eight Member States out of 25 consider their current system as not fully reliable or very reliable is evidence for the problem described. 'Moderately reliable' is not considered sufficient. When national systems are being interconnected, there needs to be also minimum harmonisation of the resilience and thus the reliability needs to be assessed as high in all Member States in the future.

www.parlament.gv.at

Results of the Commission Open Public Consultation[30] also point to a need to address existing gaps in resilience[31]. Industry feedback supports the finding that resilience gaps translate into degraded performance during crises[32]. Power outages are seen as an even stronger constraint[33]. On structural resilience, industry respondents point to the effect of limited redundancy/backup, hindering effectiveness[34].

2.2. What are the problem drivers (PDs)?

PD1 – Limited interoperability between critical communication systems, caused by cost, technological and operational complexity of interconnecting, and diverse technologies in use.

Interoperability constraints are rooted in a heterogeneous technology and uneven modernisation across Member States. Both desk research and stakeholder consultations converge on the same structural point: critical communications across Member States have evolved on different timelines and with different technical choices, resulting in systems that do not interconnect consistently across borders and between emergency services[35].

Survey evidence illustrates the extent of this diversity of technologies in use. Most Member States still operate only narrowband systems[36] and the deployment of national critical communication systems also varies widely from early deployments in the 1990s to systems introduced as recently as 2020–2024, reflecting different investment cycles and **evolution** pathways[37]. Targeted interviews showed that reasons include the lack of a European broadband alternative and lengthy contracts for narrowband technologies (going up to 20 years).

When asked specifically about 3GPP-standardised LTE/5G deployment for critical communications[38], only 9 out of 25 Member States report having already started deployment, while a substantial number of Member States plans deployment only in later timeframes, including 5 out of 25 Member States only targeting 2036[39]. This is due to the lack of funding and a harmonised European framework. The resulting heterogeneity and fragmentation results in practice in limited

---

[30] The Commission Open Public consultation - although helpful to confirm certain assumptions - is in fact much less a basis for the assessment than the elements mentioned above and must not be confused with the surveys conducted by the independent study.

[31] Feedback received from secunet Security Networks AG, Telefonica SA, Verisure Group, the Confederation of European Security Services (CoESS), and the Firefighters of Madrid Municipality.

[32] Based on the industry survey answers to the question "To what extent does the network congestion due to high traffic hinder the effectiveness of cross-border critical communication systems during crisis situations?".

[33] Based on the industry survey answers to the question "To what extent do the power outages hinder the effectiveness of cross-border critical communication systems during crisis situations?".

[34] Based on the industry survey answers to the question "To what extent do the absence of redundancy or backup systems hinder the effectiveness of cross-border critical communication systems during crisis situations?".

[35] Informal Commission Expert Group on Mission Critical Communication (MCCG), *Opinion 1/2025: Plan for Developing the European Critical Communications System (EUCCS)*, Version 1.0 (8 May 2025).

[36] Based on the survey question "What is the technological evolution or maturity level of your country's current national critical communication system?": 13 out of 25 Member States still operate narrowband-only systems (TETRA/Tetrapol), while the remainder report hybrid configurations combining narrowband with some form of broadband (trials).

[37] Based on Member States answers to the survey question "Since when has/have your existing national critical communication system(s) been in operation?".

[38] 3GPP is the backbone of modern mobile communications, laying the foundation for seamless connectivity through its rigorous standardization process.

[39] Based on the Member States answers to the survey question "Has your country designed, implemented, or begun deploying a broadband network based on 3GPP-standardised LTE and/or 5G technologies for critical communications?".

www.parlament.gv.at

interoperability. Even within Member States, interoperability between different types of emergency services is not universal[40]. Cross-border interoperability is significantly less developed[41].

Respondents also identified technical barriers, meaning the incompatibility of its equipment and services, within TETRA and Tetrapol standards as obstacle to interconnection, followed by the financial and operational burden of sustaining interconnection arrangements[42]. Interview outcomes reinforce this finding. The consulted EU institutions and agencies, national authorities, end-user organisations and industry actors consistently point to interoperability – both cross-border and cross-agency - as one of the most critical shortcomings affecting cooperation and incident response.

Limited interoperability due to incompatible technologies and varying levels of system maturity emerges as the most important problem driver in the Commission Open Public Consultation, pointed out by 88% of respondents[43].

PD1 has a causal link with P1, since the limited interoperability between Critical Communication Systems leads, in practical terms, to limited cross-border operational mobility and communication between emergency services.

PD2 - Insufficient network coverage in certain areas of Member States, specifically border regions.

Coverage limitations are a structural constraint, particularly in border areas and sparsely populated regions. Even where systems achieve high coverage, stakeholders note that operationally relevant coverage is not evenly distributed: Rural and remote areas can face a weaker signal, limited capacity and fewer resilience features, while coverage near borders may be intentionally reduced or engineered conservatively to manage interference risks. This can create “dead zones” of degraded service where cross-border deployments and mutual assistance are most likely to be needed.

Survey results indicate that most respondents consider overall coverage to be strong, but a non-negligible minority still report gaps, suggesting that baseline coverage remains uneven across Europe, as the Nordic countries reported for example in the Mission Critical Communication Group that they face more pronounced coverage constraints[44].

Stakeholders emphasise that coverage remains a key operational determinant. Where connectivity is weak, responders must rely on workarounds and operate with reduced situational awareness, therefore cross-border cooperation becomes more difficult. The practical complexities of ensuring reliable coverage in border regions, where spectrum coordination and interference management can constrain how networks are configured and where seamless handover cannot be assumed, have been identified. In the Commission Open Public Consultation, a significant share of respondents points to

---

[40] Member States‘ answers to the question “To what extent does/do the current national critical communication system(s) support technical interoperability between public safety and emergency services within your country?”: 13 out of 25 Member States report “fully interoperable” and 5 out of 25 “mostly interoperable”, while 7 out of 25 report only moderate to no cross-agency interoperability.

[41] Based on the survey question “To what extent does/do the current national critical communication system(s) in your country support technical interoperability with critical communication systems in other EU Member States?”: 11 out of 25 report cross-border interoperability is significantly less developed.

[42] Based on the answers to the survey question “What are the main barriers to establishing such interconnections?”.

[43] Member States report systems are “not interoperable at all” with neighbouring Member States, and only 2 out of 25 report full cross-border interoperability.

[44] 18 out of 25 Member States rate coverage as excellent (>90% geographic or >95% population coverage), and a further 3 out of 25 rate it as good. However, 4 out of 25 report only moderate coverage.

www.parlament.gv.at

insufficient network coverage in certain areas (68%, 17 out of 25 respondents). Uptake of satellite-based solutions to increase coverage remain limited.

PD2 also contributes to P1 because weak coverage means public authorities in charge of security and safety cannot rely on seamless connectivity when operating in border, rural and remote regions, which, in turn, limits operational mobility.

PD3 – Fragmentation of governance models, roles, responsibilities and operating procedures during crises, as well as inconsistent legal frameworks across agencies and national systems.

Governance, operational, and legal fragmentation remain a constraint[45]. Desk research underlines that operational mobility depends on more than technical connectivity: It requires alignment of legal, organisational and semantic dimensions, yet EU and Schengen-wide standard operating procedures are absent, and existing arrangements are often bilateral, or case-specific[46].

Survey results indicate uneven preparedness to manage crises, specifically across borders. Only 8 out of 25 Member States report having operational procedures in place to support cross-border missions and collaboration, while the others do not have such procedures, have not confirmed them, or report that they are not applicable in practice[47]. In the absence of a common operational framework, public authorities in charge of security and safety continue to rely on ad-hoc arrangements and bilateral agreements to communicate and cooperate, often leading to suboptimal operational outcomes in cross-border emergencies. While governance of critical communication systems is reported as centralised in most cases (20 out of 25 Member States), responsibility for managing critical communications is typically spread across several bodies (ministries, agencies and, in some cases, state-owned operators or contractors), and a minority of countries also involve regional and local entities, creating coordination requirements during crises[48].

Two-thirds of respondents to the industry survey identify fragmentation in the governance of critical communication systems across Member States as a main current challenge. Moreover, a majority of industry respondents (5 out of 9) assess that fragmented governance and coordination between authorities hinder the effectiveness of cross-border critical communications, indicating that governance gaps are not only a public-sector concern[49]. Fragmentation of governance frameworks,

---

[45] Inter-operability is only partly a technical problem. It remains entirely true that TETRA and Tetrapol are technologies that can only be integrated with significant effort. However, the main reason inter-operability was never systematically pursued and thus not achieved across the EU is the lack of a governance that could manage the complexity of aligning technical dimensions, operational procedures, harmonisation of minimum requirements and investment cycles. The three Nordic countries succeeded also because cross-border cooperation in security and safety matters is based on a very specific culture of trust and cooperation that cannot be replicated simply between all Member States. Only EU-level action will be able to establish EUCCS. This is similar to other complex initiatives in the security and telecommunication domains: the Schengen Information System, the Entry-Exit-System, the introduction of a common charger or the end of roaming charges for commercial customers are examples where *technically* Member States, or the market, could have tackled a specific problem, but only EU-level governance and regulatory powers made it possible in the end.

[46] Informal Commission Expert Group on Mission Critical Communication (MCCG). Report from the Working Group on "Standard Operating Procedures" (SOP), Version 1.0 (29 May 2024).

[47] Based on the EU Member States survey answers to the question "Do you have operational procedures in place to support cross-border missions and collaboration between authorities from different EU Member States?".

[48] Based on the EU Member States survey answers to the question "How is the governance of the national critical communication system(s) organised in your country?".

[49] Based on the Industry survey answers to the questions "What are the main challenges your organisation faces in current cross-border critical communication systems? Select all that apply." and "To what extent do the fragmented governance and coordination between authorities hinder the effectiveness of cross-border critical communication systems during crisis situations?".

www.parlament.gv.at

roles and procedures across agencies and Member States is also identified as a key constraint in the Commission Open Public Consultation (84% of respondents).

Problem Driver 3 feeds Problem 1 because fragmented governance, standard operating procedures and legal frameworks prevent consistent authorisation and coordination across agencies and borders, limiting operational mobility and inter-agency communication.

PD4 – The developments of cellular technology in commercial communications raise the expectations about the functionalities that emergency services should have access to beyond what legacy systems can deliver.

PD4 concerns a widening capability and expectation gap driven by rapid advances in commercial cellular communications. Adaptation to new communication technologies is traditionally more cautiously pursued by emergency services, because reliability and ensured functionality are the most important requirement. Mass-market smartphones, fourth and fifth generation mobile networks (4G/5G) and mainstream applications have normalised real-time, content-rich communications (images, video, location and data), and this increasingly shapes what emergency services consider necessary. However, many critical communication systems still rely primarily on narrowband, which cannot provide routine, data-intensive use.

Stakeholder evidence consistently points to rising operational demand from emergency services for richer functions such as sharing images and video, improving situational-awareness tools and collaborating in real time[50]. Interviewees point out that the personnel of emergency services sometimes compensate for the lack of these functionalities through parallel personal smartphones and consumer applications, which creates security risks. Video and large data transfer are currently missing. This translates into basic things like live video-feeds during operations, as well as the lack of the ability to integrate data from sensors like those monitoring position and vital signs, or vehicles, such as drones and CCTV systems.

Therefore, there is a growing demand to transition to 3GPP-based broadband systems, which would enable mission-critical services beyond voice, including mission-critical data and video delivered over 4G/5G networks.PD4 links directly to P2, as commercial cellular evolution is raising the baseline of what "functional" critical communications look like, and legacy systems cannot meet those expectations.

PD5 – Existing security standards, technologies and infrastructures are insufficiently adapted to address evolving threats.

The threat environment for critical communications is evolving faster than national systems. Legacy narrowband systems benefit from a non-IP-based architecture that provides intrinsic protection against certain cyber threats, but these technologies are 25 years old. In 2023, the "TETRA:BURST" report revealed a set of vulnerabilities in TETRA networks, including a weak cryptographic scheme that enables attackers to de-anonymise and track users[51].

Industry respondents report that cybersecurity vulnerabilities hinder cross-border critical communications during crises at least "to a certain extent"[52]. This finding is supported also by

[50] Feedback from operational trials of the EUCCS Preparation Project.
[51] Midnight Blue, The TETRA:BURST Vulnerabilities (2023) https://www.midnightblue.nl/research/tetraburst.
[52] Based on the Industry answers to the survey question "To what extent do the cybersecurity vulnerabilities hinder the effectiveness of cross-border critical communication systems during crisis situations?": 4 out of 9 at least "to a certain extent" and 1 out of 9 report "to a great extent" or "always".

www.parlament.gv.at

feedback given by emergency services via the Commission Open Public Consultation[53]. Respondents to the Commission Open Public Consultation highlight limitations in existing security standards and infrastructures are a major challenge (76%, 19 out of 25 respondents).

Desk research points to a regulatory gap. There is currently no applicable EU legal act that addresses comprehensively the resilience of systems used for mission-critical communications as a sector. Horizontal instruments such as NIS2 Directive[54] and CER Directive[55] set obligations for the digital infrastructure sector, but critical communication systems are excluded from their scope[56]. At the same time, relevant EU cybersecurity initiatives, notably the 5G Cybersecurity Toolbox[57], do not yet fully translate into harmonised, mission-critical requirements and assurance practices across the diverse national configurations used for public safety and security[58]. However, the recently proposed Digital Networks Act[59], provides for an obligation for providers of public electronic communication networks, and publicly available electronic communication services to take all necessary measures to ensure uninterrupted availability of critical communications[60].

PD4 directly feeds P3, as evolving threats that outpace existing technologies and related security standards and practices contribute to reducing the resilience of critical communication systems.

PD6 - Dependence on a single national mission-critical network with no assured alternate network to use in case of disruption.

Member States' narrowband networks have no assured alternate network to use in case of disruption. Recent natural disasters show that critical communication systems can suffer cascading disruption when power, backhaul and site autonomy are simultaneously stressed[61].

Because there is generally no secondary mission-critical network, a national outage can rapidly become a single point of failure for command-and-control and responder safety. In contrast, 3GPP standards for mission critical services treat mission-critical communications as an application and service layer that runs on dedicated servers and is accessed over a mobile network. This architecture

---

[53] Feedback received from the German Police Trade Union, the Ministry of Justice and Digital Affairs of Estonia, the Government of Canary Islands, and the Firefighters of Madrid Municipality.

[54] Directive (EU) 2022/2555, https://eur-lex.europa.eu/eli/dir/2022/2555/2022-12-27/eng.The NIS2 Directive does not apply to EUCCS and Member States' critical communication systems, since it excludes as per Article 2 *'public administration entities that carry out their activities in the areas of national security, public security, defence or law enforcement, including the prevention, investigation, detection and prosecution of criminal offences.'* On the other hand, the minimum requirements for national critical communication systems under Policy Measure 2.6 will be coherent with and inspired by NIS-2 and the CER-Directive.

[55] Directive (EU) 2022/2557, https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng.

[56] Informal Commission Expert Group on Mission Critical Communication (MCCG), Workgroup on Security

[57] European Commission, *The EU toolbox for 5G security* (29 January 2020) https://digital-strategy.ec.europa.eu/en/library/eu-toolbox-5g-security.

[58] Impact assessment study team. Co-creation Workshop #1 on the Intervention Logic. (02 October 2025).

[59] Proposal for a Regulation on Digital Networks COM(2026) 16 final.

[60] The proposal for a Digital Networks Act (DNA) includes provisions linking to the envisaged EUCCS Regulation. The DNA was drafted in coherence with EUCCS and states '*The Commission will adopt in 2026 a proposal to establish the European Union Critical Communication System (EUCCS), to be operational by 2030, that will provide broadband based secure communication services for public authorities across the EU and the Schengen area. The DNA proposal complements those efforts by contributing to the EU's overall capacity to respond to security threats and crises.'* Recitals 29, 38, as well as Articles 5 and 9 of the DNA proposal are designed to pave the way to Policy Measures described in this draft impact assessment report, including PM 2.6 and 2.8.

[61] For example, Ireland's official post-incident review of Storm Éowyn reports that TETRA base station sites were impacted by infrastructure damage or power loss, and that some services experienced significant disruption and loss of voice capability in the worst-affected areas.

www.parlament.gv.at

can guarantee higher resilience because the same mission critical service can, in principle, be reached via more than one underlying mobile network operator network. This is in line with stakeholder findings, as most respondents to the industry targeted survey report that the absence of redundancy or backup systems hinders effectiveness to at least a certain extent[62], and the interviews with the Mission Critical Communication Group explicitly point to the need for multi-operator resilience.

PD6 directly contributes to P3, because reliance on a single mission-critical network with no assured operational alternative translates into reduced resilience.

2.3.How likely is the problem to persist?

Problem 1. Limited operational mobility

All signs point toward this problem persisting and worsening. It is possible to make these assumptions based on the overall fragmentation and uneven technological maturity observed across Member States. Without EU action, the legal framework for mission critical communications would remain fragmented, with significant disparities between Member States and disparities in investment cycles, governance models and national priorities. Thus, operational mobility is not achieved, while the need for it continues to rise.

Observing the rising trend of cross-border emergencies, as shown for example by the increasing number of requests of cross border intervention by fire authorities[63], it is likely that this trend will continue. Consequently, emergency services would continue to lack effective means to communicate in cross-border and inter-agency missions, negatively affecting their ability to effectively tackle cross-border missions.

Problem 2. Limited functionality of legacy systems

All signs point toward this problem worsening. The telecommunication world is marked by rapid technological change. In the commercial sphere, transfer of video and large data is a reality since a long time, allowing also for a dynamic ecosystem for the development of applications and solutions. The gap between what is available in the commercial and business world compared to what current narrowband critical communication systems allow for is increasing with each new broadband-based innovation. It is one of the reasons that emergency services are in many cases forced to switch to commercial solutions that are neither designed, not equipped for critical communication purposes.

The reliance on narrowband creates a gap between law enforcement and malign actors, given the latter ones can easily adopt the latest commercial solutions, or even tailor-made communication solutions for criminal purposes. Developments related to Artificial Intelligence, Internet of Things, satellite connectivity and quantum will only widen the gap of what current narrowband can offer, compared to what is needed and expected by emergency services to effectively conduct their missions.

---

[62] Based on the industry answers to the survey question "To what extent do the absence of redundancy or backup systems hinder the effectiveness of cross-border critical communication systems during crisis situations?": 5 out of 9 Member States report that the absence of redundancy or backup systems hinders effectiveness to at least a certain extent.

[63] For instance, in 2025 there were 29 wildfires in Portugal in which Spanish firefighting resources were deployed, and 14 wildfires in Spain in which Portuguese resources were deployed. Data is available at https://www.proteccioncivil.es/documents/20121/0/Informe%20anual%20de%20incendios%20forestales%202025/e21875ac-6eec-9ef0-3bc8-06227b443bcb.

www.parlament.gv.at

Problem 3. Insufficient resilience

All signs point toward this problem persisting, moreover it is likely to worsen. The strategic framework of the EU rests on the assumption that challenges both in terms of man-made hazards, including ones stemming from geopolitical confrontation, as well as the impact and frequency of natural hazards are likely to increase[64].

As described above, communication infrastructure has specific requirements for ensuring its resilience. Without action being taken that would also accelerate the transition of critical communication systems towards broadband, those systems would not benefit from the concrete advantages in terms of resilience that broadband offers (redundancy, dynamic environment for threat detection and mitigation, continuous innovation in the commercial sphere, back-up solutions via non-terrestrial assets etc.). Furthermore, the communication world is moving towards broadband fast and narrowband technologies will not enjoy the same level of innovation and maintenance. In case narrowband would be maintained, the problems with its resilience would worsen over time, given that there are less providers of security solutions, encryption and less experts for maintenance.

3. WHY SHOULD THE EU ACT?

3.1.Legal basis

The initiative shall enable emergency services to carry out their operations across the EU and Schengen area. This can only happen based on common requirements, rules and procedures which are **legally binding** and **directly applicable** in all Member States.

The legal bases of the legislative proposal are Articles 87 and 196 of the Treaty on the Functioning of the European Union (TFEU). Article 87(2) TFEU provides a legal basis for the establishment of EUCCS for public security authorities, notably law enforcement, border guards, customs. The legislative proposal should be intended as a further development of the Schengen acquis. Article 196 TFEU provides a legal basis for public safety authorities, notably firefighters, civil protection and rescue services. For legal reasons, two separate legal instruments would be required to cover all emergency services. Other users, notably armed forces, other public authorities or operators of critical infrastructure can be included by national decision. However, there is no obligation stemming from the EU legal act.

3.2.Subsidiarity: Necessity of EU action

The principle of subsidiarity is described in Article 5(3) TEU.

Over the past few years, Member States have experienced increasingly frequent and more severe natural and man-made disasters. Disasters such as the Covid-19 pandemic, catastrophic floods of July 2021 affecting Germany, Belgium and the Netherlands, or the Iberian Peninsula blackout in April 2025. Crises affecting more than one Member State and requiring joint response are the new normal. Member States acknowledge thus the need for EU action: the Mission Critical Communication Group endorsed in 2025 the **EUCCS Operational Plan** to facilitate the task of coordinating the establishment of EUCCS. There are thus strong involvement and constant consultation with Member States, which requested action by the Commission on EUCCS, including by proposing a legal basis.

---

[64] See *ProtectEU: a European Internal Security Strategy* COM(2025) 148 final (Brussels, 2025) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025DC0148 and *European Preparedness Union Strategy*, JOIN(2025) 130 final.

www.parlament.gv.at

Also in relevant Council working parties, as well as at the level of the Council itself, Member States had asked for the establishment of EUCCS for many years [65].

Furthermore, the study highlighted that one of the key challenges affecting the current situation of critical communications across the EU is the existence of varying levels of technological maturity of critical communication systems across the EU[66]. Given that these systems evolve from different baselines, shaped by different budgetary capabilities, procurement cycles, and national risk appetite[67], the transition toward advanced technologies is progressing at an uneven pace.

Given that EUCCS will cover the whole of the EU and the Schengen area and will need to rely on a set of binding common rules, there is no realistic alternative to EU action. In the absence of such action, Member States would need to engage in a very large number of bilateral and multilateral agreements, operational procedures and technical arrangements, assuming they would still pursue the goal of interconnecting their next generation mission critical communication systems.

3.3.Subsidiarity: Added value of EU action

Subsidiarity (For non-exclusive competence)

The Union's action can be considered more effective than what Member States acting alone can do, as it can establish a harmonised EU framework facilitating cross-border and interagency critical communications. Completing EUCCS for the whole of the EU and Schengen area by 2036 will directly benefit the operations of around five million members of emergency services in Europe to save lives and prevent harm to health and property, presenting one of the highest added values.

EUCCS will streamline the costly deployment of mission-critical broadband and thus create benefits for adequately planning of human and financial resources. Assuming all Member States are completing the transition to broadband by 2036, Member States remain responsible for covering the costs for their national systems. Several Member States (e.g. France, Finland) are currently allocating national funding for this purpose, using also EU funding such as the Recovery and Resilience Facility. Other Member States indicated in the Mission Critical Communication Group that they would seek EU financial support to transition to mission critical broadband. Such funding could easier be part of the future EU funding programmes, if it corresponded to a legal obligation.

When measuring the added value of EU action, it is important to consider that the technical basis for EUCCS is the result of cooperation of the Commission, Member States and European industry. The components of the system have been developed and tested by Member States' stakeholders, notably around 100 emergency services to validate that the solution creates added value. The surveys conducted clearly show that Member States expect that the creation of EUCCS will address current challenges in cross-border critical communication:

Figure 3: Reported level of expectation for the EUCCS to address current challenges in cross-border critical communications[68]

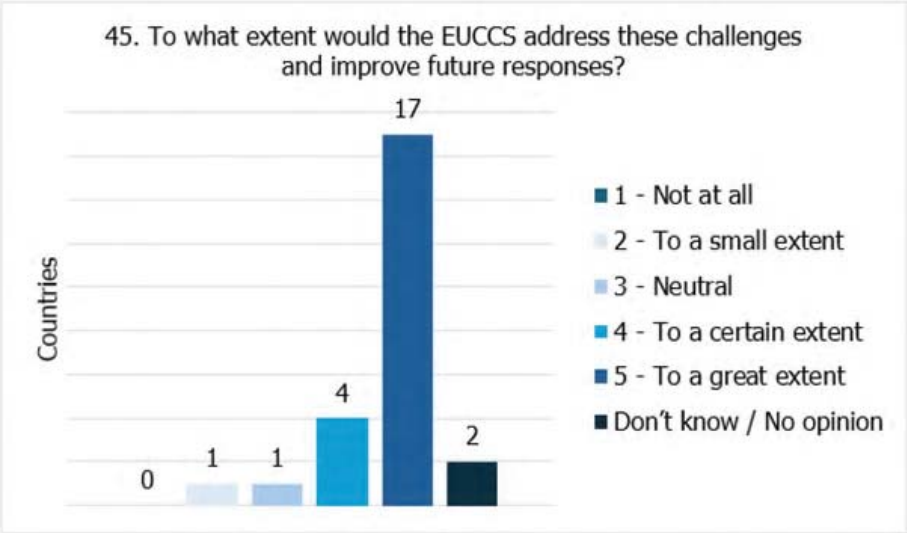
---

[65] Council Conclusions 9545/21 on the Protection of Public Spaces (2021); Council Recommendation (EU) 2022/915 on operational law enforcement cooperation (2022);.

[66] Targeted interview with MCCG Working Group for Action 5: Alignment of National Components (11 December 2025).

[68] Based on the survey answer to the question "To what extent would the EUCCS address these challenges and improve future responses?".

www.parlament.gv.at



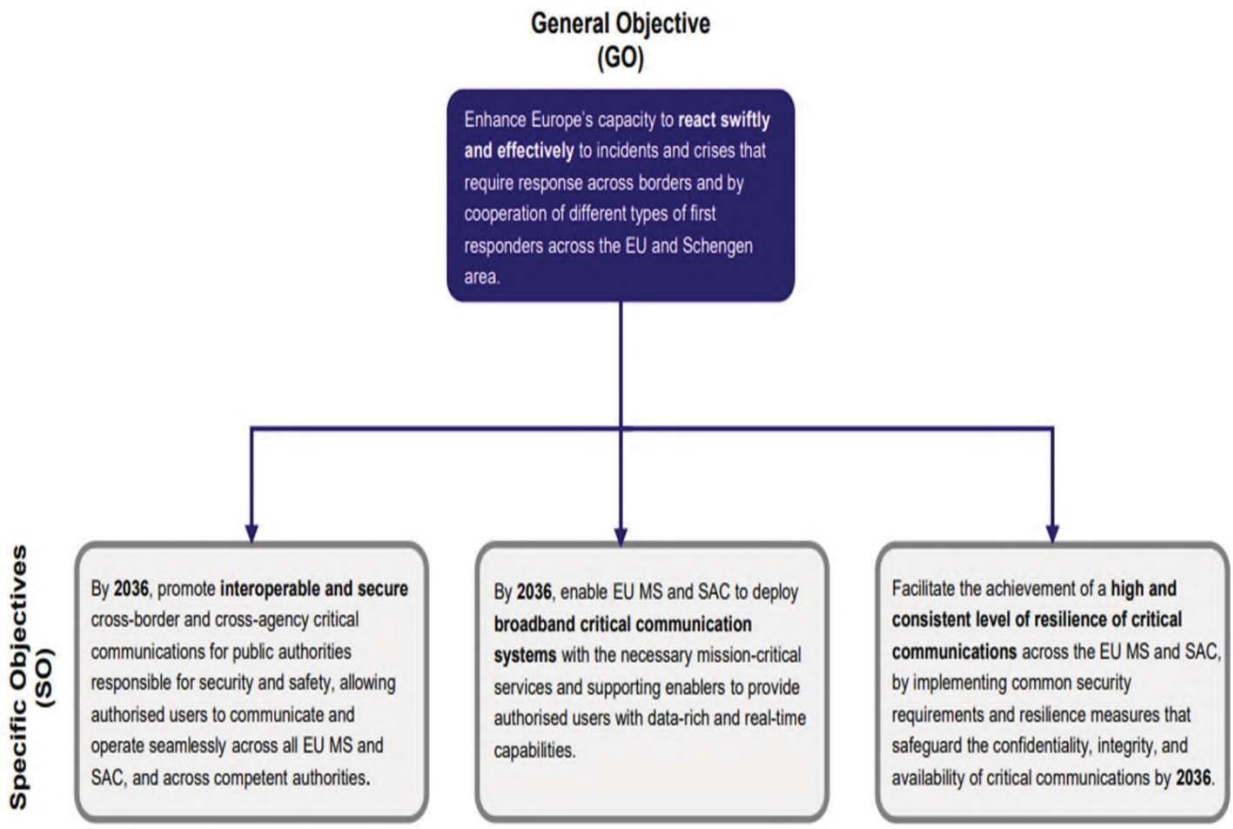
4. OBJECTIVES: WHAT IS TO BE ACHIEVED?

4.1.General objective

The general objective is to enhance Europe's capacity to react swiftly and effectively to incidents and crises that require response across borders and by cooperation of different types of emergency services.

Figure 4. Objective tree

www.parlament.gv.at



4.2.Specific objectives

The specific objectives have been identified as in line with other EU policies:

4.2.1 SO1: Promote interoperable and secure cross-border and cross-agency/operator critical communication and operational mobility among emergency services.

The objective is to provide for emergency services a resilient critical communication infrastructure that enables seamless operational mobility promote interoperability and strengthen cross-border and cross-agency operational mobility for an enhanced emergency response[69]. Specifically, all the critical communication systems of law enforcement, civil protection, and other emergency response services across Member States need to be harmonised and interconnected.

Successful implementation of SO1 will be measured by the number of Member States that have interconnected critical communication systems, providing cross-border and inter-agency critical communication. This will be assessed in three stages: 2030, 2033, and2036.

4.2.2 SO2: Support Member States to deploy broadband critical communication systems

The ability to exchange data-rich information, such as images or video, across borders and in real time was highlighted as a central reason for the upgrade of the current legacy systems used, notably TETRA. Most of the Member States (17 out of 25) report a planned upgrade of their national legacy

[69] *White Paper: How to Master Europe's Digital Infrastructure Needs?* (2024)

www.parlament.gv.at

narrowband systems[70]. There is no contradiction between the upgrade of narrowband systems and the transition to broadband. All critical communication systems in Member States will run for a certain time in a hybrid setting, in which TETRA and mission-critical broadband will run in parallel. This is called the 'migration phase' in which user groups shift step by step from TETRA to broadband networks. It is important to underline that it is not EUCCS that 'replaces' TETRA. It is the technological shift to broadband that will phase out narrowband technologies, like it has done already in commercial telecommunication.

Targeted interviews point to the need of transition to broadband to allow for the deployment of interoperable 5G mission-critical capabilities. Broadband communications technology satisfies the current and evolving needs for increasing data consumption, supporting advanced functionalities, such as real time incident reporting, high-resolution Geographic Information System (GIS), and high bandwidth data exchange (i.e., live video, biometric data), and facilitating the integration of Artificial Intelligence. In this regard, interviewees also underlined the role of harmonisation at technological level in making national investment in critical communications more attractive, while supporting the development of a more integrated and technologically advanced European critical communications ecosystem overall.

To conclude, a consensus is observed as to the necessity to transition to broadband as this would ensure that critical communication systems remain technologically robust, reliable, and future-proof, able to adapt to new technologies and develop new capabilities.

Successful implementation of SO2 would be measured by the number of Member States who deployed mission critical broadband systems as well as the total number of emergency services' personnel that are connected to those systems.

4.2.3 SO3: Facilitate the achievement of a high and consistent level of resilience of critical communications across Member States

Resilient infrastructure is needed to ensure connectivity and availability in all circumstances. In this context, resilience refers to the capacity of critical communication infrastructures to withstand, absorb, and rapidly recover from natural and man-made threats. Notably this can be achieved by ensuring advanced backup power, redundant coverage, separation of mission critical core network and radio access network as well as protocol and cryptographic security. In terms of security a broadband system would improve encryption and authentication allowing for stronger protection against cyberattacks. Resilient critical communication systems can thus be achieved by progressively strengthening the robustness of national critical communication systems through common resilience and security baselines and the deployment of advanced protective measures at EU level. Survey findings indicate that further action at the EU level would strengthen the overall resilience of national critical communication systems[71]. Furthermore, achieving this specific objective would contribute to future-proofing critical communication systems, increasing Europe's strategic autonomy in cases of geopolitical developments that harm EU interests. Successful implementation of SO3 would be

[70] Member States may furthermore decide to run TETRA systems for longer periods to have a proven and widely available back-up solution for voice communication, which remains the single most important type of communication that must not fail during an emergency.

[71] Based on the industry survey answers to the question "To what extent would the EUCCS provide greater resilience of critical communication?", with 3 out of 9 industry respondents considering that it would do so "to a certain extent" and another 3 out of 9 "to a great extent".

www.parlament.gv.at

measured by the compliance of Member States to the commonly agreed minimum resilience requirements[72].

5. WHAT ARE THE AVAILABLE POLICY OPTIONS?

5.1. What is the baseline from which options are assessed?

The baseline scenario is that there have been very few successful implementations of interconnecting emergency services' networks across borders, as well as limitations to critical communication between different types of emergency services.

The legal framework for mission critical communications is fragmented as no harmonisation takes place. On the technical side and despite project-level achievements, significant disparities between Member States exist that continue to depend on narrowband systems as their primary national critical communication systems, and those Member States who introduced complementary broadband services. 13 out of 25 Member States still operate narrowband-only systems (TETRA/Tetrapol), while 12 Member States report hybrid configurations combining narrowband with some form of broadband (trials). Technological dependence on third countries in critical communication is today low. Not a single Member State is dependent on a third-country provider for their core network. While there are important suppliers of non-EU origin, there is no systemic dependency problem, given that alternatives in Europe are available. The aim is at least indirectly to maintain such level of autonomy, while having to consider the realities in the global digital communication market. There are limits on what an initiative establishing EUCCS can do to address systemic dependencies in the commercial digital infrastructure and telecommunication sector.

Consequently, emergency services that rely on an outdated technical solution frequently revert to unsatisfactory ad hoc arrangements, or commercial solutions unfit for critical operations to communicate. Effective operational cooperation between services and across borders is significantly limited by that.

5.2. Description of the policy options

Starting from this baseline, three possible policy options have been considered. The table below presents the intervention logic by showing what problem each policy option is addressing and what it is expected to achieve.

Figure 5: Intervention logic

[72] As defined in the EUCCS Operational Plan and later to be adopted by an Implementing Act (see policy measures).

www.parlament.gv.at

Pillar I - Rationale of the Intervention

Problem Drivers (PD)

PD1 – Limited interoperability Limited interoperability between critical communication systems, caused by cost, technological and operational complexity of interconnecting, and diverse technologies in use.

PD2 – Insufficient network coverage
Insufficient network coverage in certain areas of EU MS, specifically border regions.

PD3 – Fragmented governance
Fragmentation of governance models, roles, responsibilities and operating procedures during crises, as well as inconsistent legal frameworks across agencies and national systems.

PD4 – Evolution of cellular technologies
The developments of cellular technology in commercial communications raise the expectations about the functionalities that public authorities responsible for security and safety should have access to beyond what legacy systems can deliver.

PD5 – Security standards not adapted to evolving threats
Existing security standards, technologies and infrastructures are insufficiently adapted to address evolving threats.

PD6 – Dependence on a single network
Dependence on a single national mission-critical network with no assured alternate network to use in case of disruption.

General Objective (GO)
GO - Enhance Europe's capacity to react swiftly and effectively to incidents and crises that require response across borders and by cooperation of different types of emergency services across the EU and Schengen area.

Specific Objectives (SO)
SO1 – By 2036, promote interoperable and secure cross-border and cross-agency critical communications for emergency services, allowing authorised users to communicate and operate seamlessly across all EU MS, and across competent authorities. This objective is directly linked to PD1 and PD3.
SO2 – By 2036, enable EU MS to deploy broadband critical communication systems with the necessary mission-critical services and supporting enablers to provide authorised users with data-rich and real-time capabilities. This objective is directly linked to PD2.
SO3 – Facilitate the achievement of a high and consistent level of resilience of critical communications across the EU MS, by implementing common security requirements and resilience measures that safeguard the confidentiality, integrity, and availability of critical communications by 2036. This objective is directly linked to PD4, PD5 and PD6.

Problems (P)
P1 – Limited operational mobility Existing critical communication systems in the EU enable only limited operational mobility of emergency services across borders and limited communication between agencies, not fully taking into account evolving threats and growing interoperability needs and further exacerbating the fragmented governance scenario.
P2 – Limited functionality of legacy systems Narrowband critical communication systems do not support data-rich capabilities already available to civilians and expected for the increased efficiency of operational response, thus not fully taking into account the evolution of cellular technologies and further complicating operations in case of insufficient network coverage.
P3 – Insufficient resilience Insufficient resilience of critical communication systems across the EU and Schengen area, especially where there is no operational alternative to the single systems in place in the EU. This is further exacerbated by the dependence on a single network.

Pillar II – Policy Options

Policy Options (PO)

- **PO0 - Status quo**: no EU legislative framework governing critical communication systems; EU MS would continue to develop and operate their critical communication systems independently. This PO would not address any of the PD: PDs would persist in the absence of any EU action.
- **PO1 – Voluntary pursuit of technical interconnectivity**: issuance of non-binding guidance encouraging EU MS to voluntarily improve cross-agency interconnection and cross-border cooperation. This PO would partially address the PDs: in the case of PD1 for instance, this option would perhaps lead to the pursuit of partial interoperability between MS systems for voice communication.
- **PO2 – Establishment of a 'system of systems'**: adoption of an EU legal act providing the legal basis enabling the interconnection of EU MS critical communication systems while preserving sovereignty. Each EU MS keeps its own servers under its own jurisdiction while ensuring standards-based interoperability with the EUCCS, with mission critical services and cross-border emergency response. Implementation would take place gradually: an initial phase connecting around eight to ten EU MS by 2030, followed by the progressive expansion of services and country participation in 2033 and 2036. Two sub-options are foreseen at EU level to monitor and verify the EU MS readiness to connect to the EUCCS and manage the technical, operational, and administrative aspects of the EUCCS:
  - PO2.1 - decentralised EU governance
  - PO2.2 – EU competent authority

Both, PO 2.1. and 2.2 would address all PDs successfully.

Pillar III – Expected Impacts

Expected Outputs (EO)
EO1 - Adoption of minimum technical and operational requirements for national critical communication systems to ensure interoperable critical communication systems (PO2; PM2.6). This would contribute to ER1 and ER2.
EO2 – Adoption of appropriate standard operational procedures for critical communications by national authorities responsible for critical communication systems, in coordination with relevant EU bodies (PO2; PM 2.11 + 2.9). This would contribute to ER3.
EO3 – Establishment of Member States' competent authorities and harmonised governance architecture (PO2; PM 2.1). This would contribute to ER4.
EO4 – Establishment of EU-level governance architecture (PO2; PM 2.1 + 2.2 + 2.4).This would contribute to ER4.
EO5 - Establishment of the European Critical Communication Committee (ECCG) (PO2; PM 2.1). This would contribute to ER4.
EO6 - Requirement for EU MS to interconnect the EUCCS (PO2; PM 2.5). This would contribute to ER4.
EO7 - Requirement that Mobile Network Operators guarantee access and service to critical communication (PO2; PM 2.8). This would contribute to ER5.
EO8 – Development of reporting and monitoring mechanisms to track progress against national strategies (PO2; PM2.3). This would contribute to ER5.
EO9 – Development of reporting and monitoring mechanisms to track compliance with the EU legislative act (PO2; PM 2.7). This would contribute to ER5.
EO10 – Creation of coordinated training, education programmes and exercises for emergency services (PO2; PM 2.12). This would contribute to ER5.
EO11– Standard Operating Procedures Handbook to be developed by ECCG (PO1; PM 1.4 & PO2; PM 2.11). This would contribute to ER5.

Expected results (ER)
ER1 – Enhanced operational mobility across borders and agencies for emergency services. This would contribute to EI1, EI2 and EI3.
ER2 – Increased resilience of EU MS national critical communication systems. This would contribute to EI1, EI2 and EI3.
ER3 – Increased operational efficiency of EU MS critical communication systems. This would contribute to EI1, EI2 and EI3.
ER4 – Progressive development and deployment of new or upgraded critical communication infrastructures, devices, applications and services, stimulating the continuous evolution of critical communication systems. This would contribute to EI1, EI2 and EI3.
ER5 – National critical communication systems can respond to evolving user needs and technological innovations. This would contribute to EI1, EI2 and EI3.

Expected impacts (EI)
EI1 – Enhanced EU-wide preparedness and coordinated crisis response against natural or man-made disasters, terrorist and cross-border crimes, and armed conflicts through secure, reliable, and interoperable critical communication systems that support coordinated action by all relevant emergency services.
EI2 – Positive social impacts, including greater citizen trust, safety, security and civil protection across EU MS enabled by faster, more coordinated and effective emergency responses, ultimately resulting in saving lives.
EI3 - Positive environmental impacts, including earlier detection with faster and better coordinated cross-border responses to natural disasters, thereby reducing environmental damage.

Pillar IV- External Factors

External Factors (EF)
EF1 - The EU and Schengen area are expected to experience extreme events, exposure and vulnerability to natural disasters due to climate change.
EF2 - Evolving, hybrid threats increase security risks for the EU and Schengen area if not effectively mitigated.
EF3 - Heightened geopolitical tensions and global economic uncertainty affect Europe's technological sovereignty and supply chain stability.
EF4 - EU MS are subject to extraterritorial access laws of third countries.

www.parlament.gv.at

5.2.1. Policy option 0: no further EU intervention

PO0 assumes the case of no EU intervention, meaning that the scenario described in the baseline would persist. While market-driven or voluntary initiatives could promote cooperation between Member States' critical communication systems, such developments have not materialised in the last decades and would remain unlikely in the absence of a coordinated European approach. Furthermore, the costs for the necessary upgrades to modernise national critical communication systems to broadband would continue to be borne entirely by Member States individually, without any coordinated investment and financial support at EU level. Under PO0, fragmentation between Member States' critical communication systems is projected to increase, given the uneven technological maturity across Member States.

5.2.2. Policy option 1: voluntary pursuit of technical interconnectivity

PO1 is based on voluntary measures to promote interconnection of critical communication systems between Member States. This would include the publication of non-binding guidance by the Commission. Similarly to PO0, Member States would continue to develop their national critical communication systems independently. They would either maintain narrowband systems or transition to broadband solutions, in line with national strategies, priorities, and available resources.

PO1 is addressing in principle all problems and their drivers. However, given the voluntary nature it is extremely unlikely that all Member States and all emergency services would participate in a 'voluntary EUCCS'. The survey launched with Member States concludes that only eleven Member States would be willing to work on interoperability of broadband systems in the absence of a binding EU framework. Thus, while PO1 in theory aims at all problems and their drivers, it is very unlikely to solve any of them in a satisfactory manner. The assumption is further substantiated by the fact that the initial approach in the BroadMap and BroadWay projects (2016 – 2022) was based on a voluntary approach that should lead to a coordinated procurement of inter-operable solutions. It is to a significant extent the experience from that project which led to the common understanding of Member States and the Commission services that only an approach based on binding EU-level rules is likely to successfully establish EUCCS.

In PO1, the Mission Critical Communication Group would recommend relevant international standards (e.g. those developed by the European Telecommunications Standards Institute or 3GPP) and promote common operational procedures to support interconnection among participating Member States. EU funding of projects could be leveraged aligning to existing priorities. PO1 would include those measures, which may be taken entirely or selectively:

<u>PM1.1 - Continuation of the mandate of the Mission Critical Communication Group as an informal expert group</u>

The Commission would renew the Mission Critical Communication Group mandate, maintaining it as expert group with an advisory role to support its work on interconnectivity, standards, the modernisation and innovation of national critical communication systems, and on voluntary interconnection between Member States. It would also contribute to the development of non-binding working documents, including guidance on standards for critical

www.parlament.gv.at

communication systems interconnection and security as well as the EUCCS Standard Operating Procedures Handbook.

PM1.2 - Promotion and guidance on standards for interconnectivity and security

This PM promotes the consistent adoption and implementation of standards, notably those developed by the European Telecommunications Standards Institute and 3GPP, to enable technical interconnectivity among Member States. The Commission, supported by the Mission Critical Communication Group, would ensure awareness, encourage adoption of relevant standards.

PM1.3 – Exchange of best practices on critical communication systems modernisation and innovation

This PM facilitates the exchange of best practices between Member States in transitioning from narrowband systems to broadband-based solutions that meet evolving operational and security needs of critical communications. Through the Mission Critical Communication Group, Member States would share and consolidate technology-neutral approaches on phased-in migration strategies, the adoption of broadband technologies for critical communications, and the incorporation of innovative features such as secure data exchange and need resilience mechanisms.

PM1.4 – Development of an EUCCS Standard Operating Procedures Handbook

This PM develops a voluntary EUCCS Standard Operating Procedures Handbook to support Member States in harmonising operational procedures under the EUCCS framework. Coordinated by the Mission Critical Communication Group, the Standard Operating Procedures Handbook would define common operational procedures – including a common taxonomy for Member States and guidance on governance, roles and responsibilities, and crisis workflows, and it would serve as reference for aligning national Standard Operating Procedures with best practices in critical communications at EU-level.

PM1.5 – Recommendations on resilience of critical communication systems infrastructure

This PM foresees non-binding recommendations to Member States, issued by an EU body in collaboration with the Mission Critical Communication Group, notably relating to cybersecurity and hybrid threats to strengthen the resilience of national critical communication systems infrastructure. These recommendations would provide a common ground of guidance and examples of technical and functional improvements, gathered through peer exchange, to enhance preparedness against cyberattacks and hybrid threats, this way reducing major disruptions, and improving the overall resilience and security of critical communication systems across Member States.

5.2.3. Policy option 2: legislative proposal establishing a system of systems

PO2 includes the adoption of an EU legal act providing a legal basis for the establishment of a decentralised EU framework (i.e., a ‘system of systems’) enabling the interconnection of Member States national critical communication systems while preserving Member States’ sovereignty over their national critical communication systems.

www.parlament.gv.at

The legal act would set out objectives, roles and responsibilities, minimum technical requirements, and cross-border procedures. Implementation would take place gradually following a convergence period with an initial system connecting around eight to ten Member States by 2030, followed by a progressive expansion of services and participation in 2033 and 2036.

At the EU-level, there would be no central data management infrastructure or central operations capacity but a governance, as well as common support functions for Member States' systems. Interconnection of Member States' systems will be facilitated, and a central EU level monitoring capacity will be established. The combination of those elements is the EU-level component of EUCCS.Two sub-options exist that differentiate from each other according to the level of centralisation of this EU-level component:

- In sub-option 2.1 the **EU-level component is light** with a stronger role of the Member States, for which the current EUCCS Preparation Project will be reinforced to become the EUCCS Cooperation Project and only the necessary elements for facilitating interconnectivity, monitoring and support tasks being handled at EU-level.

- In sub-option 2.2 there is a central **EU competent authority** that covers tasks related to facilitation on technical interconnectivity, common EU services as well as monitoring of the implementation of EUCCS across Member States.

The EUCCS framework would be in principle the same under both sub-options, thus also the Policy Measures to be taken under the sub-options are identical:

I. Governance and strategy

PM2.1 – Establishment of governance structures at the Member State and EU levels, as well as of an European Critical Communications Group Committee

This PM establishes a governance architecture through the EU legislative act to ensure coordinated implementation, consistent decision-making, and clear accountability. More specifically:

- Designation of a National Competent Authority[73] as the Member States' EUCCS single point of contact. The National Competent Authority would oversee the development, implementation, and operation of national mission critical broadband system and services, ensure security and resilience, and enable interoperability and cross-border cooperation, including EUCCS testing, field exercises and reporting processes. Each National Competent Authority would need to appoint a Single Point of Contact for coordination with other National Competent Authorities;
- Establishment of the European Critical Communication Group as formal expert group to advise the Commission (replacing the existing informal Mission Critical Communication Group). The European Critical Communication Group would be tasked to ensure EU- and Schengen-wide coordination and provide structured input through comitology to steer implementation priorities and support the EU in adopting implementing and delegated acts.

[73] Informal Commission Expert Group on Mission Critical Communication (MCCG) Working Group on Action 5. *National Competent Authority Tasks for EUCCS Services.* Working document, Version 009 (4 December 2025).

www.parlament.gv.at

Its delegates come from the National Competent Authorities of Member States[74]. The governance is the same as other formal Commission expert groups. Furthermore, several other policy measures are going to be guided and adopted by the group.

PM2.2 – EU-level monitoring of compliance and maturity assessment via a System Accreditation Board

This PM establishes a System Accreditation Board comprising of delegates from Member States to assess the progressive maturity of national critical communication systems in line with the EUCCS, including notably if a Member State is ready to join EUCCS. It would build on the EUCCS maturity approach (Traditional → Initial 2030 → Advanced 2033 → Optimal 2036)[75]. Its activities would cover the verification of national critical communication systems interconnection, roaming readiness, rollout of baseline mission critical services and key enabling capabilities, as well as alignment with the EUCCS security and resilience expectations, notably recognised cybersecurity management practices and the progressive uptake of European Telecommunications Standards Institute/Global Certification Forum standardisation and certification[76]. Maturity assessment would be conducted through a structured peer-review process using objective and proportionate criteria and evidence, ensuring comparability. For legal reasons, the function of the System Accreditation Board cannot be performed by the European Critical Communication Group (or any other comitology committee).

PM2.3 - Member States' strategies on critical communications

This PM obliges Member States to adopt and maintain an EUCCS strategy/roadmap aligned with the EU legislative act and the EUCCS Operational Plan. This would mirror the approach taken in frameworks such as NIS2 and ensure political ownership, planning certainty, and accountability. The strategy/action plan should set out: (i) national governance (including designation of the National Competent Authority and national points of contact for cross-border cooperation and interoperability testing), (ii) implementation timelines and milestones for procurement, rollout and migration to mission critical broadband and mission critical services, (iii) investment priorities and financing, (iv) an approach for the transition from legacy narrowband systems (including their role and interoperability during migration, if it's the case), and (v) national risks with mitigation measures (security, resilience, continuity, and preparedness). Member States would be responsible for keeping the strategy updated over time.

---

[74] This concerns notably: PM 2.3 (*Member States' strategies*) where the group will be the key forum to discuss those strategies; PM 2.6 (*Minimum requirements for national critical communication systems*), for which the group will support the Commission in the drafting of an Implementing Act (see also further below); PM 2.7 (*Reporting obligations for Member States*), where the group will be the key forum to discuss reports received by the Commission; PM 2.9 (*Adherence to risk-based guidance concerning autonomy and sovereignty)* to serve as forum for exchanges of best-practices and exchanges with relevant other stakeholders, including industry; as well as PM 2.11 (*Standard Operating Procedures*) to be adopted by the group.

[75]See EUCCS Operational Plan p. 20-21. The governance and operations of PO 2.1 are based on findings of the EUCCS Operational Plan and the results of the EUCCS Preparation Project in which Member States, emergency services and industry partners work since many years on the technical and organisational backbone of EUCCS, including the maturity model.

[76] Mission Critical Communication (MCCG) Working Group on Action 5. *EUCCS System Initial Maturity Level 2030 Definitions.* Working document, Version 005 (21 January 2026).

www.parlament.gv.at

II. EU-level components and system support function

PM2.4 - Creation of the European Network Monitoring Centre and European Security Monitoring Centre

This PM mandates the creation of an EU-level technical and component that provides the initial interconnection functionality for the Member States' systems and ensures high-level monitoring of the Member State networks. An IP interconnection exchange to facilitate interconnection of critical communication systems and monitoring of transmission capabilities shall be operated by a **European Network Monitoring Centre.** It does not, however, include operation or central data management; thus development, maintenance and operations of critical communication remain under full Member State control.

A **European Security Monitoring Centre** will be created to receive and review reports and issue recommendations or corrective actions on security incidents that affect Member States' critical communication systems. It does not handle security incidents itself but acts as monitoring capacity.

Following good practice from the telecommunication sector and related policy domains, the Network Monitoring Centre and Security Monitoring Centre are going to be separate entities. They will be set up by the European Commission, likely using framework contracts to designate a specialised commercial service provider.

PM2.5 – Establishment of the interconnection of EU and national components of EUCCS

This PM establishes that Member States must connect their national critical communication systems within a defined transition period. Interconnection would be based on common standards and agreed technical profiles to ensure end-to-end interoperability verified prior to connection to the EUCCS against conformance testbeds hosted by the European Network Monitoring Centre. The testing would verify technical, operational, and administrative conformance of the connected national critical communication systems against the established standards. Each Member States would retain jurisdiction and operational control over its infrastructure and servers. At the same time, interconnection would be mandatory to guarantee operational mobility and seamless cross-border communications.

PM2.6 – Minimum requirements for national critical communication systems

This PM sets minimum technical and operational requirements for national critical communication systems to ensure interoperable critical communication systems both within and across Member States. That will be achieved via testbeds: Member States would need to ensure that their national systems meet the requirements for connecting to EUCCS against those testbeds.

Detailed technical parameters would be specified and updated through implementing/delegated acts and through the EU standardisation and certification process (European Telecommunications Standards Institute/European Committee for Standardisation/European Committee for Electrotechnical Standardization) that would translate the EUCCS Operational Plan into common specifications and testable profiles. EUCCS and the Member States' systems are based on the mission-critical standards developed in 3GPP, with a supplementary EUCCS-centred standard being developed in Europe by ETSI.

www.parlament.gv.at

The minimum requirements to be adopted via and Implementing Act concern also the resilience and security of the Member States' systems[77]. Detailed parameters that are likely to inspire the drafting of that Implementing Act are included in the EUCCS Operational Plan[78]. Other technical parameters necessary to successfully interconnect Member States' systems and ensure the compatibility of different devices and services are to be achieved via the adherence to standards (3GPP and ETSI).

III. Requirements of critical communication systems

PM2.7 – Reporting obligations for Member States

This PM sets obligations for Member States and operators of critical communication systems to periodically report to the EU to support EU level oversight and the EUCCS maturity assessment. Reporting would cover the progress in meeting the minimum requirements set by the EU legislative act, the implementation of national strategies/action plans, operational performance and reliability metrics, compliance with security and resilience requirements, including significant incidents/vulnerabilities and mitigation measures and adherence to the EUCCS Standard Operating Procedures Handbook. Reporting will be done only every two years, and the Commission will provide a common format (template or electronic platform).

PM2.8 – Obligations for Mobile Network Operators to support critical communication

This PM introduces a requirement for Mobile Network Operators in the EU legislative act to guarantee access and service to critical communication users on national networks, coherent with the obligation already proposed in the Digital Networks Act. These obligations would ensure that critical communications receive priority over commercial traffic in duly justified cases, especially during crises. As critical communication is delivered via Mobile Network Operators or other commercial networks; these obligations should cascade to the contractual and regulatory arrangements between Member States and the Mobile Network Operators.

PM2.9 – Adherence to risk-based guidance concerning autonomy and sovereignty

This PM embeds autonomy and sovereignty as guiding principles of the EUCCS framework. It does not set rigid obligations; instead, it establishes common expectations for governance and operation of national critical communication systems, reflected primarily in the recitals of the EU legislative act. It promotes maintaining Member States jurisdictional control over core network functions and sensitive operational data by limiting external dependencies through risk-based vendor and supply-chain choices for critical components, with mitigation where sovereignty or security risks arise. It is ensuring consistency with existing and forthcoming EU initiatives (e.g., NIS2, Cloud & AI Development Act, the 5G Cybersecurity Toolbox).

PM2.10 – Establishment of the EU support functions of the EUCCS

[77] Besides the resilience requirements to be specified in an implementing act, the envisaged legal act under PO 2.1 will also include an article on resilience of Member States' systems under which they will need to ensure resilience and protection measures for their critical communication systems.
[78] A summary of chapter 7.2.2 of the EUCCS Operational Plan is provided in Annex 7.

www.parlament.gv.at

At EU-level, there will be further support to Member States' critical communication systems. To address *PD2 - Insufficient network coverage* and *'PD6 - Dependence on a single national mission-critical network with no assured alternate network to use in case of disruption'* the EU satellite constellations, such as IRIS², will be leveraged to support EUCCS. While EUCCS (and critical communication is general) relies primarily on terrestrial networks, satellites have a crucial role for back-up and additional coverage. The planned use of IRIS² for EUCCS was announced 2023 in the EU Space Strategy for Security and Defence and has been detailed out in a dedicated working team of the Mission Critical Communication Group. Satellite connectivity is a key component and indeed EUCCS is the main driver within IRIS² for the development of direct-to-device functionalities. There is full complementarity with the EU satellite programme and the future use of direct-to-device communication in included into EUCCS, since critical communication on broadband will be a mix of land-based and space-based connectivity. Technical preparation talks have been conducted, and a concept of operations will be proposed. A future trial of EUCCS in 2027 would test the use of EU satellite connectivity to provide additional back-up (if land-based communication systems are disrupted) and coverage (in areas where there is no mobile network). In the future, Member States connected to EUCCS will thus have the possibility to use tokens for their critical communication purposes and deploy satellite support.

IV. Support measures for operations

PM2.11 – Standard Operating Procedures Handbook

This PM mandates the European Critical Communications Group to develop binding EUCCS Standard Operating Procedures. The procedures would ensure predictable cross-border cooperation by harmonising how authorities request and aid, coordinate command and control, and mobilise and use EUCCS services in routine and crisis scenarios. The core elements would cover the minimum operational baseline needed for operational mobility, including a common taxonomy, common addressing, cross-border contact and escalation procedures, dispatch/control-room cooperation and information sharing, and common principles for different types of missions. The European Critical Communications Group would maintain the Handbook over time, updating the binding elements where and expanding the best practices based on joint exercises, lessons learned, and operational experience.

PM2.12 – Training, education and exercise programmes

This PM establishes Member States coordinated training, education programmes, and regular exercises[79]. The goals are to ensure emergency services can effectively operate EUCCS services and applications, improve trust, familiarity, and uptake, support the integration of new technologies, and strengthen cross-border coordinated operations. In parallel, funding has been reserved under Horizon Europe for the further technical development of EUCCS. For the EUCCS to be future proof, a continuous innovation cycle shall be run in parallel via the future EU framework for research and via the EUCCS Cooperation Project included in the preferred PO 2.1.

[79] The training is to be offered by the EUCCS Cooperation Project and addresses all emergency services personnel, as in principle all of them could be deployed in cross-border settings.

www.parlament.gv.at

Differences between Policy Option 2.1 and 2.2

As described above, the measures taken under both sub-options are identical, given they are both based on a system of systems approach. The key difference between the sub-options lays in the handling of certain tasks and monitoring. Under the sub-option 2.1 the central monitoring and facilitation of interconnection (PM 2.4, 2.5) will be set up by the Commission and outsourced under existing framework contracts to specialised providers experienced in providing such services to public authorities. The EUCCS Cooperation Project would be increased financially to provide services to Member States to support PM 2.2, 2.11 and to implement PM 2.12.

Sub-option 2.2 would foresee an EU Agency handling tasks related to central monitoring and interconnection, as well as providing common services and applications, training and further technical development. Concretely, the Agency would have performed largely PM 2.4, 2.5 and 2.12. Furthermore, it would advise on PM 2.2, 2.9 and 2.11. A graph detailing the functioning of Policy Option 2.1 is attached in Annex 7[80].

5.3. Options discarded at an early stage

Policy Option 3 would have foreseen a centrally managed EU critical communication system providing critical communication across the EU and the Schengen area, including central data management infrastructure. This centralised system would have dedicated infrastructure or establish an EU level mission critical core within the network infrastructure of commercial mobile network operators of all Member States. It would be developed and maintained by an EU institution or agency responsible for the operation, maintenance, and security of the centralised network and its shared services, including a central talk group patching capability. Given the lack of the existence of an EU body that would have the legal and operational mandate for such task, it would have required the creation of a new, dedicated EU body or agency.

It is likely that this option would have addressed P1, P2 and P3. This option was however discarded as being disproportionate, too costly and operationally unrealistic. This solution does not correspond to the operational and technical reality of critical communication which runs over mobile communication networks in a highly decentralised structure. From a system architecture perspective, centralising the connections of millions of emergency services and hundreds of thousands of base stations across 31 participating Member States is not realistic, as confirmed early on by the Mission Critical Communication Group and the EUCCS Preparation Project. A central system would as well as present a very strong interference in Member States's sovereignty. Under this option, the total costs would amount to € 13, 897 billion to be covered by EU budget, as the Union would have to cover both the EU component and Member States' costs for setting up their national broadband critical communication system (see further below costs for other PO).

Policy Option 4 would have introduced a legislative proposal to create a system of systems of the existing narrowband (TETRA and Tetrapol) systems. Such option would not have required Member States to transition into mission critical broadband, thus presenting a more harmonised starting point, given narrowband systems exist in all Member States today. In principle,

[80] See Annex 7, figure 16.

www.parlament.gv.at

interconnection of those systems would increase operational mobility for voice communication, thus serve partly P1. However, the option was discarded for two main reasons: a) it would not have addressed the problems of limited functionalities (P2) and insufficient resilience (P3), given the limitations of the current technology that were described in this impact assessment; and b) the complexity of achieving interoperability ex-ante is too high compared to paving the way for interoperability of mission critical broadband systems. As described above, existing systems cannot simply be interconnected. Investing in 2026 in interconnection of narrowband systems[81] would furthermore not be aligned with the overall Commission ambition to promote broadband across the telecommunication sector.

[81] The cost estimates for setting up (CapEx) such a single interconnection amounts to € 1,2 million. The operational costs for the ISI network between Finland, Norway and Finland amounts to € 20 million per year. In several Member States, the TETRA and Tetrapol networks are coming to their end-of-life and need either to be upgraded or replaced.

www.parlament.gv.at

6. WHAT ARE THE IMPACTS OF THE POLICY OPTIONS?

6.1.Social Impacts

The main social impact is enhancing emergency services' ability to save lives and to protect people's health, safety as well as preventing damage to private or public property. This is enabled by their increased ability to communicate seamlessly, therefore enhancing their cooperation and coordination.

PO1 generates limited social impact, as its policy measures remain confined to participating Member States. Therefore, achieving interoperable critical communication at Member State and European level would at least take very long. That means that significantly less people would benefit from faster and more efficient response by emergency services.

Social impacts of PO2.1 and PO2.2 are expected to be much higher. Both sub-options are expected to contribute significantly to the social impacts described, as the consistent deployment of interoperable critical communication will allow all people in all Member States to benefit from the fast and efficient response of emergency services.

Findings from the surveys support this assumption, with most industry respondents considering that the EUCCS would enable more efficient operations[82]. 12 out of 14 respondents in targeted interviews emphasised the added value of the EUCCS would lie in enabling seamless cross-border and cross-agency communication, improving coordination of operational responses, and ensuring timelier detection and management of crises. Responses to the Commission Open Public Consultation also confirm a clear preference for a system of systems as here foreseen in sub-options 2.1 and 2.2.

6.2.Economic Impact

Complete and fully comparable country-specific cost data are not available for all Member States. National critical communication systems differ in terms of technological maturity, governance structures and implementation pathways, which affects the comparability of some cost assumptions. While consultation and expert evidence made it possible to identify several expected benefits, not all of these could be quantified within the scope of the impact assessment[83]. The methodology applied for the cost estimates is the same used for the study provided by the external contractor[84].

---

[82] Based on the industry survey answer to the question "To what extent would the EUCCS provide more efficient operations to respond to cross-border natural or man-made disasters and security incidents?".

[83] These limitations were addressed through triangulation across evidence sources, the use of proxy values where justified, and the application of ranges or sensitivity-oriented assumptions where precise estimates could not be established. The use of a shortlisted country sample, cluster-based extrapolation, and validated interview follow-up was intended to improve the robustness of the cost model while remaining proportionate to the evidence available.

[84] The cost assessment measured incremental costs against the baseline scenario, that is, the additional costs arising under each policy option relative to continuation of the status quo. The analysis distinguished between adjustment costs and administrative costs, with costs separated into one-off (CapEx) and recurrent components (OpEx). A 7-year time horizon was chosen to mirror the phased roll-out of the EUCCS delineated in the Operational Plan, which foresees implementation milestones in 2030, 2033 and 2036. Recurrent costs were then expressed in

www.parlament.gv.at

For all policy options, it is important to differentiate between a) the modernisation of Member States' critical communication systems; and b) the costs related to establishing EUCCS. The costs for the transition of Member States' systems to broadband is not stemming from the EUCCS initiative itself or the proposed legislation. Member States have in most cases already started this process to close the technological gap that are presented by narrowband systems , and leverage innovation in telecommunications sector which are already widely available for commercial users. The transition to broadband is happening in all spheres of telecommunication at different pace to accommodate for the need of large data transfers. . Without EUCCS, this transition to broadband would only take longer, without following common timelines and standards. Furthermore, Member States deciding to maintain their narrowband communication systems would face high maintenance costs[85]. Further details on the cost data collection and estimation approach are provided in Annex 7 on the "Methodology for the cost assessment, and a detailed breakdown of costs per policy option can be found in Annexes 7.2 to 7.5.

The cost estimates have been established through extensive consultations with Member States and targeted questionnaires with European industry. A detailed breakdown of costs can be found in *Annexes 7.2 to 7.5*.

6.2.1. Policy option 0: no EU-level intervention

Under this option, Member States independently transition from narrowband to broadband solutions, following divergent strategies, priorities, and available resources. Thirteen[86] Member States, which are currently preparing for developing and setting up their broadband communication systems, provided detailed cost estimate. The costs of the status quo (PO0) comprise only the Member States' public authorities' related costs, given that under this policy option, there is no EU-level intervention.

On this basis, cost estimates for the other Member States were calculated, by dividing them into three groups of large, medium-sized and small Member States:

1) Cluster 1 consists of eight large Member States: **France, Romania, Spain, Sweden**, Germany, Italy, Norway and Poland.

2) Cluster 2 consists of fourteen medium-sized Member States: **Belgium, Czech Republic, Denmark, Finland, the Netherlands**, Austria, Bulgaria, Greece, Hungary,

---

present-value terms using a 3% social discount factor in real terms. Nothing indicates that the initiative would increase the costs of the Member States in terms of the Cost data for EU-level public authorities were estimated based on working meetings conducted with the European Commission and technical experts. The absence of incremental costs for businesses and other economic operators has been confirmed through targeted interviews as well as working meetings with the European Commission and relevant business associations and industry representatives.

[85] Finland signed a 10-year contract for € 48 million with its primary mobile network operator in 2020. 2028-2030 is the deadline for migration to broadband, with TETRA phasing out in 2032. The annual costs for TETRA till 2032 amounts to € 25,8 million. For keeping TETRA beyond 2032, investments of up to € 50 million per year would be needed.

[86] Belgium, Czech Republic, Denmark, Estonia, Finland, France, Latvia, Luxembourg, the Netherlands, Romania, Slovenia, Spain, and Sweden.

www.parlament.gv.at

Ireland, Lithuania, Portugal, Slovak Republic, Switzerland (including Liechtenstein, which will share one system with Switzerland).

3) Cluster 3 consists of eight smaller Member States: **Estonia, Latvia, Luxembourg, Slovenia**, Croatia, Cyprus, Iceland and Malta.

Member States marked in **bold** provided detailed cost estimates for PO0 as well as for sub-options PO2.1 and PO2.2 which were the basis for the calculations presented in Annexes 7.2, 7.4 and 7.5.

The estimated costs for establishing the national broadband critical communication systems (capital expenditure/CapEx) range from € 70 million for Estonia and € 231, 9 million for Belgium to € 410 million for France. The estimated operational expenditure/OpEx costs per year is € 14 million for Estonia, € 75,3 million for Belgium and € 101 million for France.

As shown in *Annex 7.2*, the average capital expenditure costs per year amount to € 292 million for a large, € 122 million for a medium-sized and € 55, 9 million for a large Member State. The average OpEx costs per year amount to € 67, 4 million for a large, € 48, 1 million for a medium-sized and € 12, 16 million for a small Member State. Calculated over a seven-years period, the total investment for setting up all the Member States' broadband critical communication systems amounts to **€ 12, 667 billion**[87].

6.2.2. Policy option 1: Voluntary pursuit of technical interconnectivity

Eleven Member States (Austria, Sweden, France, Finland, Germany, France, Finland, Germany, Poland, Italy, Ireland, Norway, Iceland, Lithuania) replied that they have (as it is already the case for Finland, Sweden and Norway participating in the FINOSE-ISI cooperation) respectively are planning or willing to create interconnections with two or more neighbouring countries. Six Member States gave a negative reply and eight replied that they do not know. Only those eleven Member States that expressed an interest to establish bilateral connections were considered for estimating the costs for PO1.

Annex 7.3 gives an overview of the estimated costs for PO1: For Member States, the average costs for setting up one bilateral connection (CapEx) are estimated to amount to € 1, 4 million. The estimated costs for maintaining this connected over 7 years amount to € 1, 18 million. At EU level, the cost estimates for the continuation of the mandate and management of the Commission expert group on mission critical communication over seven years and for the elaboration of guidelines amount to € 3, 38 million.

The **total estimated costs for PO1** amounts to **€ 162, 44 million**, consisting of the costs for voluntary interconnectivity of the above mentioned eleven Member States, considering the number of interconnections they envisage (ranging from one to eight), and of EU costs.

6.2.3. Policy option 2: legislative proposal establishing a system of systems

PO2 foresees a 'system of systems' enabling the interconnection of Member States national critical communication systems, with sub-option 2.1 foreseeing a lighter EU-level component

[87] This considers that Liechtenstein will be part of the Swiss national system.

www.parlament.gv.at

and sub-option 2.2 envisaging a central EU competent authority facilitating this interconnection.

The cost estimates for **PO2.1**, consisting of costs for Member States and costs for the EU, are presented in *Annex 7.4*: The **Member States' costs** amount **to € 2, 415 billion**, consisting of **adjustment costs** for network, infrastructure, user equipment, applications and software licences for connecting to the EUCCS ecosystem, as well as of **administrative costs**, consisting of reporting tools for the national competent authority, human resources needed for reporting and statistical work, training, etc. The detailed cost estimates provided by the thirteen Member States listed above provided the basis for calculating the costs for all Member States, following the cluster-approach.

The **EU costs** amount to **€ 1, 156 billion**, covering costs for the dedicated Internetwork Packet Exchange (IPX) network, standardisation and certification, satellite connectivity, testbeds, the European Network Monitoring Centre, the European Security Monitoring Centre, the European Critical Communications Group Committee, the System Accreditation Board, the tasks of the EUCCS Cooperation mechanism, the elaboration of standard operating procedures and guidelines, additional human resources and for training of staff. The **total costs for sub-option 2.1** are estimated to amount to **€ 3, 571 billion**.

The cost estimates for **PO2.2** can be found in *Annex 7.5:* Covering the same cost items, the **Member States' costs** for PO2.2 are the same for PO2.1, amounting to **€ 2, 415 billion**. The EU cost estimates for PO2.2 are slightly lower than for PO2.1, amounting to **€ 1, 153 billion**. This is due to a higher degree of centralisation, with the EU competent authority taking over the tasks of the European Security Monitoring Centre, the European Network Monitoring Centre, the System Accreditation Board and EUCCS Cooperation foreseen in PO2.1. The **total estimated costs for PO2.2** to amount to **€ 3, 568 billion**.

PO2 generates significant economic impacts, requiring substantial public investment to establish an interoperable EU and Schengen-wide system of systems. The legally binding framework enables medium- to long-term benefits, including opportunities for economies of scale through standardisation and joint procurement, and a more integrated and predictable market environment.

6.2.4. Obligations and compensation for mobile network operators

In EUCCS, mobile network operators should treat separately the critical communication traffic and users from commercial network services, ensuring quality of service, including priority mechanisms, and seamless roaming (with voice, video and data) across different mobile networks. In practice, this requires neither additional network capacity nor new functionalities, as they are already included as a basic feature in the mobile network operators' radio access networks. To meet 3GPP requirements for mission-critical services, each mobile network operator needs to configure and enable these capabilities.

Furthermore, it is worth noting that priority mechanisms that priority mechanisms do not have significant impact for commercial users under normal network conditions, as the impact is limited only to the situation when the network is overloaded. This situation only occurs seldom,

www.parlament.gv.at

leading to a temporary and usually short reduction in quality of service[88]. Operators already manage similar prioritisation for 112 calls as a standard procedure. In the Commission Open Public Consultation, one European mobile network operator which already provides mission-critical communication services via a dedicated core network pointed out that traffic prioritisation should be carefully measured and controlled to minimise impact on commercial users.

Mobile network operators may need to prioritise emergency services network traffic. This already happens today and is included into the price offer to emergency services. While the percentage of emergency services to the total number of mobile network users is less than 1%, they represent a large single customer. In a competitive market environment, they can secure a price very close to the avoidable cost level plus a reasonable margin.

This approach is illustrated by two Member State examples: a Member State established a commercial framework with two mobile network operators providing quality of service, priority and pre-emption capabilities, while national roaming agreements are in place with two additional operators, offering extended coverage. The costs related to mobile network operators are covered in the contracts and amount to € 150 million over a four-year period. Traffic prioritisation is not identified as a cost driver, but part of the service package. A second Member State signed a similar 10-year contract for € 48 million with its primary mobile network operator in May 2020[89].

Therefore, there is no need for additional network capacity and the relevant capabilities already exist in commercial networks and only need to be activated, configured or contractually framed. However, actual costs may vary depending on the national implementation model and the service, resilience, security and interoperability requirements imposed. The synthesis of the information collected indicates that EUCCS is not expected to new infrastructure costs for mobile network operators, as the required functionalities are, in most cases, already embedded in commercial 4G/5G standards and infrastructures. The main economic impact relates instead to contractual service levels, resilience requirements, operational integration, and governance arrangements defined at national level. The EUCCS does not add costs for MNOs in terms of traffic because emergency services users typically represent less than 1% of total subscribers; prioritisation mechanisms are activated dynamically only during congestion situations; these situations remain infrequent and temporary; and operators already manage comparable priority mechanisms today, including emergency call handling and network management policies. Further details are provided in Annex 7.8.

In case Member States consider negotiating compensation with mobile network operators, the compensation model should be based on avoidable costs plus a reasonable margin. This approach would support economic efficiency and ensure market neutrality by preventing

[88] Based on targeted interviews with Member States in the MCCG that have already such arrangements with mobile network operators, as well as feedback from the EUCCS Preparation Project

[89] Information provided in the draft impact assessment on the obligations for MNOs is provided via dedicated interviews with technical experts from four Member States. Those Member States have contractual arrangements with Mobile Network Operators to facilitate mission-critical communication.

www.parlament.gv.at

overcompensation of a single mobile network operator. It would also avoid emergency services from being pushed to cheaper, less resilient commercial offers[90].

For Mobile Network Operators, the large-scale shift of critical communication to commercial networks offers new business opportunities. The need to grant certain priorities is well understood in the sector and consequently was not fundamentally objected in targeted consultations[91] and the open public consultation.

6.2.5. European industry

EUCCS depends on supply chains for network infrastructure, devices, applications and services. In this security relevant area, the EU and Member States should safeguard their strategic autonomy. European companies have played a key role in developing technological solutions for EUCCS in the pre-commercial procurement project BroadWay and continue this important role in the EUCCS Preparation Project. There are positive economic impacts expected for European providers of critical communication infrastructure and services due to the accelerated transition of Member States to broadband systems and reliable timelines till 2036[92].

6.2.6. Impact on SMEs and competitiveness

For the industry overall, there are positive impacts expected for providers of critical communication infrastructure and services due to the accelerated transition of Member States to broadband systems and reliable timelines till 2036. We estimate 9,000 SMEs are offered new market opportunities. Those providing existing Applications will be encouraged to become compatible with EUCCS, which is not considered to be a complex process. A dedicated SME test has been performed in Annex 6.

6.3.Impact on fundamental rights

All options would comply fully with fundamental rights considerations.

EUCCS aligns with human rights and fundamental freedoms, adhering to the principles and rights enshrined in the Charter of Fundamental Rights of the European Union (The Charter), the European Convention on Human Rights (ECHR). Specifically, the EUCCS enhances interoperability among emergency services across agencies and borders, ensuring an effective and coordinated response to security threats, crises, and the protection of citizens throughout

---

[90] Furthermore, this approach ensures strict compliance with the CJEU Altmark ruling (Case C-280/00), which dictates that compensation must not exceed what is necessary to cover costs incurred in discharging public service obligations. It also prevents wide pricing disparities across the Union, where local market conditions might otherwise distort the cost of essential safety services.

[91] The information provided in this draft impact assessment on the obligations for Mobile Network Operators is provided via dedicated interviews with technical experts from Finland, Belgium, Norway and France. Those Member States have contractual arrangements with Mobile Network Operators to facilitate mission-critical communication. A dedicated consultation was furthermore organised for Mobile Network Operators in March 2026 in DG HOME, attended the GSM Association (GSMA). Neither in reaction to this consultation, nor as part of the open public consultation have MNOs raised significant concerns related to possible obligations to facilitate critical communication.

[92] See Annex 5 and 6, based on input from the associations representing the critical communication industry (The Critical Communication Association- TCCA and Public Safety Communication Europe-PSCE, as well as the market study “SNS Telecom Public Safety Market report 2026”.

www.parlament.gv.at

the Member States. The security of every person is protected under Article 6 of the Charter and Article 5 ECHR. Under Article 2 ECHR, Article 2(1) and Article 3(1) the Charter, the EUCCS could support the protection of life as well as the physical and mental integrity of people by enabling rapid emergency response and coordination during crises such as terrorist attacks or natural disasters. EUCCS does not equip law enforcement and emergency services with any capabilities that may be used for direct exercise of force or infringements of other rights.

6.3.1 Compliance with Regulation 2016/679 (GDPR Regulation)

Under Article 8 ECHR (right to respect for private and family life), Article 7 (respect for private and family life) and Article 8 the Charter (protection of personal data), the EUCCS fully comply with the standards laid down in Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR). The EUCCS facilitates the exchange of operational data exclusively among emergency services and directly associated entities, e.g. emergency medical services, hospitals. Such exchanges may include victim-related data, such as name, age, sex, physical or psychological condition, but remain strictly limited to public security and safety purposes. These advancements serve solely to improve emergency response, without altering the existing legal framework for data protection. EUCCS on the other hand does not enhance the capabilities of law enforcement for activities with a potential fundamental rights impact, such as surveillance of private communication.

The restrictions of data subject rights (e.g. access, erasure, or objection) in cross-border data exchanges are in line with Article 23 GDPR, as the new dimension permits restrictions by way of a legislative measure when necessary for public security, national defence, or law enforcement, provided such limitations are proportionate. For critical communication, processing of personal data would be based on the vital interest to protect life and to prevent serious threats.

6.4. Impact on the environment

EUCCS will have positive impacts on the environment, notably as it enhances the capability to respond to disasters with environmental impacts such as floods, fires and industrial accidents, as well as the fight against environmental crime. PO1 generates limited environmental benefits, as it relies on voluntary uptake. However, it would still provide benefits against environmental challenges such as climate change, chemical hazards, and ecosystem degradation. While improved coordination and response in crisis situations may support the mitigation of environmental risks, impacts remain limited in scope and uneven. PO2.1 and 2.2 both generate more positive and structurally significant environmental benefits through strengthened cross-border response capacity and interoperability across Member States.

6.5. Impact on digitalisation

PO2 is expected to have a high impact on digitalisation of Public Administration and promote broadband deployment. Critical communication among emergency services and other relevant forces will contribute to digitalisation of their operations. It will also contribute to Digital Government goals, including interoperability of Public Services. For PO1 that impact would be more limited, as the roll-out of broadband for critical communication would be at least slower.

www.parlament.gv.at

6.6. Impact on vulnerable people/gender considerations

PO2 is expected to have a positive impact on vulnerable people. The possibility to exchange real-time video feeds, richer situational awareness tooling and collaborative field applications could better support emergency services in communicating with vulnerable people in distress, e.g. the possibility to exchange in real-time videos communication to support American Sign Language communication with people with hearing disabilities or allowing emergency services to live-streaming a situation of distress for elderly, child or person with disability to ensure the intervention of specialists.

7. HOW DO THE OPTIONS COMPARE?

The objective of this comparison is to determine which option performs best against a consistent set of evaluation criteria. The comparison focuses on PO1 and PO2 and their sub-options. Each policy option was evaluated against the following criteria:

- Effectiveness, i.e. the extent to which the option achieves the specific and general policy objectives of the intervention;
- Efficiency, i.e. the relationship between the resources used (costs) and the results achieved (benefits);
- Coherence, i.e. the extent to which the option is consistent with other relevant Union policies and legal frameworks;
- Subsidiarity and proportionality, i.e. whether the policy option is appropriate and does not go beyond what is necessary to achieve the policy objectives.

In addition, the analysis considers the economic, social, and environmental impacts. Policy options that outperformed others were assigned a relative “+” or “++”. Those that underperformed were assigned a relative “-“ or “--", and those that were average, were assigned a relative “0”.

7.1 Effectiveness

The table below summarises the expected effectiveness of the proposed policy options vis-à-vis the specific objectives of the intervention, namely:

- Specific Objective 1: promote interoperable and secure cross-border and cross-agency critical communications for public authorities responsible for security and safety, allowing authorised emergency services to communicate and operate seamlessly across all EU Member States, and across competent authorities.
- Specific Objective 2: enable EU Member States to deploy broadband critical communication systems with the necessary mission critical services and supporting enablers to provide authorised emergency services with data-rich and real-time capabilities.
- Specific Objective 3: Facilitate the achievement of a high and consistent level of resilience of critical communications across the EU Member States, by implementing common security requirements and resilience measures that safeguard the confidentiality, integrity, and availability of critical communications by 2036.

www.parlament.gv.at

	PO 1 - Voluntary pursuit of technical interconnectivity	PO 2.1 - system of systems (lighter EU-level component)	PO 2.2 - system of systems (central EU competent authority)
SO #1	PO 1 delivers limited improvements in interoperable and secure cross-border and cross-agency critical communications, as it relies on voluntary interconnectivity and non-binding coordination. Impacts remain uneven across Member States, with limited uptake reducing its effectiveness in ensuring seamless communication. (+)	PO 2.1 delivers significant improvements in interoperable and secure cross-border and cross-agency critical communications through binding interoperability requirements and mandatory connectivity. That binding element ensures that all Member States participate and thus more emergency services benefit from EUCCS. However, coordination across multiple governance bodies may affect the uniformity and timeliness of implementation. (++)	PO 2.2 reveal to be similar to 2.1 exception made for clearer accountability, more streamlined decision-making, and more consistent oversight. Given the centralisation of such task in an EU competent authority. (++)
SO #2	PO 1 is only marginally effective in enabling the deployment of broadband critical communication systems. The absence of binding requirements constrains progress, resulting in fragmented development and limited advancement across Member States. That would include very likely that some emergency services are not receiving broadband functionalities, or much later than others do. (+)	PO 2.1 is highly effective in enabling the deployment of broadband critical communication systems, including mission-critical services and data-rich functionalities. They will become available to almost 5 million responders in emergency services in foreseeable timelines. While the binding framework supports large-scale deployment, coordination complexity may lead to some implementation variability across Member States. (++)	*Identical to PO 2.1.*
SO #3	PO 1 provides limited improvements in achieving a high and consistent level of resilience of critical communications, as voluntary measures do not ensure the uniform implementation of security and resilience practices. This leads to uneven levels of resilience across Member States, given that different resilience measures are been taken and less priority may be assigned to them. (+)	PO 2.1 delivers strong improvements in achieving a high and consistent level of resilience of critical communications through common standards and mandatory requirements. This would ensure the resilience measures are comparable in the Member States and that their implementation is obligatory. However, fragmented governance may affect consistency in oversight and implementation. (++)	PO 2.2 reveal to be equal to 2.1, exception made for clearer accountability mechanisms due to the more centralised governance. Given the centralisation of such task in a EU competent authority. (++)

7.2 Efficiency

Efficiency assesses the extent to which the objectives can be achieved at the lowest possible cost, considering both direct and indirect impacts on stakeholders.

www.parlament.gv.at

	PO 1 - Voluntary pursuit of technical interconnectivity	PO 2.1 - system of systems (lighter EU-level component)	PO 2.2 - system of systems (central EU competent authority)
Costs	PO 1 is primarily driven by the additional costs for Member States, to the extent national public authorities decide to establish voluntary bilateral interconnections and would remain comparatively limited at the EU level. **EUR 162.4 million** would be necessary to create interconnections between Member States, on a voluntary basis. **(-)**	The costs of PO 2.1 are higher than option 1, mainly driven by the necessary implementation of an EU layer of the EUCCS, and the creation of one connection per Member State to it. The overall cost of PO2.1 (decentralised governance) is estimated at **EUR 3.571 billion**, comprising EUR 2.415 billion for EU Member States and EUR 1.156 billion at EU level. **(--)**	The costs of PO 2.2 remain in the same order of magnitude as the costs of option 2.1. The only difference being efficiency gains on human resources at EU level due to the centralised governance in a single agency. The overall cost of PO2.2 (centralised governance) is instead estimated at **EUR 3.568 billion**, comprising the same EUR 2.415 billion for EU Member States and EUR 1.153 billion at the EU level. **(--)** This PO introduces a high liability cost for the EU competent, who will be liable in the case the systems does not work properly in an emergency.
Benefits	Up to 3 million -responders and would have partial operational mobility, limited to the Member States with which their country has a voluntary bilateral connection. **(+)** Costs savings opportunities will remain low. **(0)** An estimated number of 11 countries could create between 2 and 3 bilateral connections. **(+)** PO 1 will slightly improve the resilience of critical communication systems, which will remain driven by Member States with voluntary guidance from the EU. **(0)** PO 1 would enable only a limited degree of seamless roaming. In addition, only a limited number of Member States are expected to transition to broadband in the temporal scope by 2036. **(+)**	5 million responders in emergency services would have full operational mobility across the Member States. **(++)** Costs savings opportunities such as joint procurement could be leveraged by Member States. **(+)** All Member States would be interconnected with each other. **(++)** PO 2.1 will improve the resilience of critical communication systems to some extent, with mandatory guidance from the EU. **(+)** PO 2.1 would enable only a high degree of seamless roaming. In addition, all Member States are expected to transition to broadband by2036, thus providing data-rich functionalities to emergency services. **(++)**	*Identical to option 2.1.*

7.3 Coherence

www.parlament.gv.at

Coherence examines the extent to which each policy option aligns with existing EU policies, legislation, and broader strategic objectives. The policies and strategies that appear relevant for a 'coherence' evaluation are essentially three:

- EU internal security policy, reflected in the ProtectEU strategy, the European Internal Security Strategy, which highlighted the need for more effective tools for law enforcement, including EUCCS enabling cross border communication between different authorities.
- EU telecommunication policy, and in particular the Digital Networks Act which aims to modernise, simplify and harmonise the EU framework for connectivity networks and contains provisions on the availability of mission critical communications.
- EU cybersecurity policy, especially the NIS2 Directive which establishes general reporting obligations for operators of essential services and digital services providers. cybersecurity risk-management and incident-reporting obligations.

	PO 1 - Voluntary pursuit of technical interconnectivity	PO 2.1 - system of systems (lighter EU-level component)	PO 2.2 - system of systems (EU competent authority)
ProtectEU strategy	Low level of interconnection of Member States due to the voluntary nature of the obligations. **(+)**	Strong level of interconnection of Member States with the implementation of an EU-layer. **(++)**	*Identical to* PO *2.1.*
EU telecommunication policy	PO 1, through its voluntary guidance and the work of the Mission Critical Communication Group is not likely to interfere with the provisions of the Digital Networks Act. **(0)**	The Digital Networks Act proposes to introduce obligations for providers of public electronic communications networks to ensure the continuity and uninterrupted availability of mission critical communications. **Coherent with the Digital Networks Act**, Policy Option 2.1 would enable data roaming to facilitate cross-border operations. **(+)**	*Identical to* PO *2.1.*
EU cybersecurity strategy	Under PO 1, Member States will have the possibility to follow voluntary guidance from the Mission Critical Communication Group on the resilience of national critical communication systems, including on cybersecurity. **(+)**	Under PO 2.1, mandatory guidance will be provided by the Mission Critical Communication Group on the resilience of national critical communication systems, including on cybersecurity aspects. **(++)**	*Identical to* PO *2.1.*

7.4 Subsidiarity and proportionality

Regarding subsidiarity, all three aspects laid down in article 5(3) of the TUE have been taken into consideration: (i) whether the initiative falls under an exclusive competence of the Union, (ii) whether the objectives of an action cannot be sufficiently achieved by the Member States, but (iii) can be better achieved at Union level, by reason of the scale and effects of the proposed action.

www.parlament.gv.at

Regarding proportionality, two main aspects have been considered: (i) whether the proposed options are proportionate to the objectives, i.e. they do not go beyond / fall short of what is necessary to satisfactorily address the problem / achieve the objectives; and (ii) whether the costs implied are proportionate to the expected outcome.

	PO 1 - Voluntary pursuit of technical interconnectivity	PO 2.1 - system of systems (lighter EU-level component)	PO 2.2 - system of systems (EU competent authority)
Subsidiarity	The cooperation among emergency services is not an exclusive competence of the Union. PO 1 **partially responds** to the fragmentation of national critical communication systems which limit operational mobility. This issue is not resolved by Member States. Only a very limited number of Member States have ongoing interoperability initiatives or are planning to interconnect with one or two neighbour Member States. PO 1 would **partially achieve the first objective** of the EUCCS it would coordinate the voluntary development of national critical communication systems in an interoperable manner. **(+)**	Cooperation among emergency services is not an exclusive competence of the Union. PO 2.1 **responds more effectively** to the fragmentation of national critical communication systems, thus fostering to a greater extent the operational mobility of emergency services. This issue and the insufficient functionalities and resilience of MCX services are not resolved by Member States. PO 2.1 **would better achieve the objectives** as it would mandate the development of national critical communication systems in an interoperable manner. **(++)**	Similar *to Policy Option 2.1.* However, the fact that significant tasks related to critical communication would be handled by an EU agency would slightly reduce Member States sovereignty in a domain related to national security and law enforcement.
Proportionality	PO 1 remains proportionate by allowing Member States to **retain full ownership** of their critical communication systems. When looking at the proportionality of costs compared to the achievement of the objectives, we note that PO1 has **moderate costs**. However, it only **partially responds** to the SO 1 and 3 of the EUCCS, almost not at all to SO 2. **(0)**	Under PO 2.1, the 'system of systems' enables Member States to interconnect while keeping their national critical communication systems. Costs and burden on Member States is higher. However, it remains proportionate, as binding requirements are **justified** by the scale of problems addressed, while measures are targeted and limited to what is y for interoperability and a consistent level of resilience and security. **(++)**	Cost and burden are similar to PO 2.1 and proportionate. However, the adaptation of an existing EU agency's mandate or the creation of a new one would be a significant effort. **(+)**

7.5 Social, environmental and economic impact

	PO 1 - Voluntary pursuit of technical interconnectivity	PO 2.1 - system of systems (lighter EU-level component)	PO 2.2 - system of systems (EU competent authority)
Social Impact	PO 1 generates **limited social benefits, namely on public health and public safety** through better coordination and response times	PO 2.1 generates **significant and structural social benefits** through binding interoperability requirements, and harmonised procedures.	Identical to PO 2.1.

www.parlament.gv.at

	PO 1 - Voluntary pursuit of technical interconnectivity	PO 2.1 - system of systems (lighter EU-level component)	PO 2.2 - system of systems (EU competent authority)
	during cross-border incidents. However, impacts **remain restricted** to participating Member States, resulting in uneven and limited effects across Member States. Up to 3 million personnel emergency services would have very partial operational mobility **(+)**	Mandatory interconnection improves **the scale, reliability, and consistency** of cooperation, enhancing real-time coordination, situational awareness, and joint operations across Member States for 5 million personnel in emergency services. **(++)**	
Environmental impacts	PO 1 generates **limited environmental benefits**, as it relies on voluntary uptake. While improved coordination and response in crisis situations may support the mitigation of environmental risks, impacts remain limited in scope and uneven across Member States due to reliance on bilateral arrangements. **(+)**	PO 2.1 generates **more positive and structurally significant** environmental benefits through strengthened cross-border response capacity and consistent interoperability across Member States. The binding and harmonised framework enables faster and more coordinated interventions, supporting more effective mitigation of environmental risks and limiting their escalation. **(++)**	Identical to PO 2.1.
Economic Impact	PO 1 generates **limited to moderate** economic impacts, primarily affecting public authorities through adjustment and administrative costs linked to interconnections. Costs remain relatively contained with **EUR 162 million**. Nevertheless, the non-binding nature of the intervention limits broader effects, preventing the emergence of significant market improvements or economies of scale. **(-)**	PO 2.1 generates **significant economic impacts**, requiring substantial public investment to establish an interoperable EU and Schengen-wide system of systems, with costs estimated at **EUR 3.571 billion.** However, the binding framework enables medium- to long-term benefits, including opportunities for economies of scale through standardisation and joint procurement, and a more integrated and predictable market environment. **(--)**	Similar to PO 2.1. PO 2.2 is slightly less costly than option 2.1 with **EUR 3.568 billion** of investment, as the centralisation of the EU governance framework allows for greater staff allocation efficiencies**. (--)**

The table below summarises the comparative performance of the policy options across the main evaluation criteria.

	Policy Option 1	**Policy Option 2.1**	**Policy Option 2.2**
Effectiveness	+	++	++
Efficiency	++	+	+
Coherence	+	++	++

www.parlament.gv.at

Subsidiarity	+	++	+
Proportionality	0	++	+
Social Impact	+	++	++
Environmental impacts	+	++	++
Economic Impact	-	--	--

Overall, the comparison indicates that Policy Option 2.1 and 2.2 perform more favourably across most criteria, particularly effectiveness and coherence. Whereas policy option 2.1 performs even stronger on subsidiarity and proportionality. Policy Option 1 on the other hand demonstrates relative advantages only on efficiency, due its low cost.

8. PREFERRED OPTION

8.1.Policy option 2.1

Based on the comparative analysis presented above, Policy Option 2.1 emerges as the preferred option.

This Policy Option provides the most effective response to the identified problem, offering a comprehensive and reliable framework for achieving the policy objectives. While it may entail higher costs compared to Policy Option 1, these are justified by the significantly greater benefits and the more substantial impacts generated across economic, social, and environmental dimensions. By contrast, Policy Option 1, although less burdensome, is not expected to deliver sufficient impact to address the identified problems, limiting its overall suitability. The U.S. system FirstNet[93] for example serves emergency services across the United States. However, all emergency services join FirstNet voluntarily at their own initiative. They are also not automatically able to communicate with each other across agencies and State borders. While FirstNet is a success what concerns its relatively early roll-out and geographic coverage, the US example confirms that **obligatory rules** are more likely to achieve the objectives described in this impact assessment.

Policy Option 2.1 and Policy Option 2.2 on the other hand present very similar benefits and impacts.

Policy Option 2.1 ensures a higher degree of coherence with existing EU policies and respects the principle of proportionality, as its measures are appropriately calibrated to the scale of the challenges addressed. The creation of the governance measures and the light EU component are relatively easy to achieve.

There is a variation of the cost, as Policy Option 2.2 requires slightly less human resources at EU level due to the centralised governance structure. However, Policy Option 2.2 would have required the creation of an EU Agency, or the significant modification of an existing Agency mandate and resources, to act as competent authority. The Commission has thoroughly reviewed existing Agencies and none of them would have the necessary legal mandate to cover

[93] https://www.firstnet.com/

www.parlament.gv.at

the different first responder groups, as well as the resources and capacity to handle the EU component of EUCCS. Creation of a new Agency on the other hand would be disproportionate.

Considering these facts, 2.1 is therefore retained as the preferred Policy Option.

8.2. REFIT (simplification and improved efficiency)

This initiative is not a revision of existing legislation; therefore, a REFIT test has not been performed.

8.3. Application of the 'one in, one out' approach

This initiative is not a revision of existing legislation; therefore, the 'one in, one out' approach does not apply.

9. HOW WILL ACTUAL IMPACTS BE MONITORED AND EVALUATED?

In line with the Better Regulation Tool #43 on the Monitoring arrangements and indicators[94], this chapter identifies core indicators to measure the success of the EUCCS initiative. This way

[94] European Commission, *Better Regulation Toolbox 2023: Chapter 5 – Monitoring the application of interventions* (2023) Tool #43 'Monitoring the application of interventions' https://commission.europa.eu/document/download/fe5655c0-d3d5-4f18-87c0-ecdce5bdf1be_en?filename=BR%20Toolbox%20-%20Dec%202025%20-%20Chapter%205.pdf.

www.parlament.gv.at

it sets a framework for the monitoring and the data collection throughout the lifecycle of the initiative to oversee its progress, ensure the availability of data, and allow for the evaluation of its results hereafter.

This exercise considers contextual considerations (i.e., technological developments, geopolitical landscape, telecommunications market changes), as they can influence the EUCCS' implementation, and leverages existent data sources, including those used in the other chapters of the report. A Table[95] was created to summarise and map the proposed indicators against the specific objectives, the policy measures, sources, the possible collection methods, the responsible entity, and the suggested frequency of collection. A prioritisation is also included reflecting the following logic:

- High priority: mandatory requirement
- Medium priority: non mandatory but highly recommended
- Low priority: non mandatory requirement

The indicators serve as a basis for a final elaboration and selection from the European Commission, for use in future exercises of data collection, for example in the context of an evaluation or revision of the legal act, or in a support/thematic study.

Based on Tool #43, the indicators also meet the Relevant, Accepted, Credible, Easy, and Robust (RACER) criteria. They are Relevant as they align directly with the specific objectives of the EUCCS initiative and its overarching goal. They will be Accepted following consultation with relevant EU bodies and Member States competent authorities. They are Credible as they are formulated in a clear and unambiguous way. They are Easy to monitor as they rely on information that can be sourced through reporting from the EU Member States National Competent Authorities and relevant EU bodies (e.g. eu-LISA, ENISA), and finally, they are Robust, as they require statistics on operational data that are machine-generated, meaning less prone to error.

To measure the success and effectiveness of the EUCCS, the Key Performance Indicators in Annex 7.9 have been identified, based on the EUCCS Operational Plan endorsed by the European Commission in May 2025. By monitoring these Key Performance Indicators, the European Commission can ensure that EUCCS will effectively meet its general objective: enhance Europe's capacity to react effectively and efficiently to cross-border and cross-agency incidents and crises, through a secure and resilient critical communication infrastructure across the EU and Schengen area.

[95] See Annex 7.8.

www.parlament.gv.at

ANNEX 1: PROCEDURAL INFORMATION

1. LEAD DG, DECIDE PLANNING/CWP REFERENCES

The lead DG is the Directorate-General for Migration and Home Affairs (DG HOME) for the preparation of this initiative and the work on the impact assessment. No other DGs were associated to the initiative. The initiative is listed in the Commission Work Programme 2026.

2. ORGANISATION AND TIMING

The inter-service steering group for the impact assessment was set up on 3 December 2024 with participation of the following Directorates-General: Secretariat-General (SG), Service Juridique (SJ), Directorate-General for Budget (BUDG), Directorate-General for Communications Networks, Content and Technology (CNECT), Directorate-General for Defence Industry and Space (DEFIS), Directorate-General for Digital Services (DIGIT), Directorate-General for European Civil Protection and Humanitarian Aid Operations (ECHO), Directorate-General for Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs (GROW), Directorate-General for Justice and Consumers (JUST), Directorate-General for Health and Food Safety (SANTE), Directorate-General for Research and Innovation (RTD), Directorate-General for Taxation and Customs Union (TAXUD), the European Commission's Health Emergency Preparedness and Response Authority (HERA), and the European Commission Joint Research Centre (JRC).

The call for evidence was launched on 30 April 2025 and concluded on 28 May 2025.

The public consultation was launched on 16 January 2026 and concluded on 10 April 2026.

Targeted stakeholder consultations were conducted from 25 July 2025 to 1 June 2026.

<u>ISG meetings:</u>

Four ISG meetings and two written consultations were organised:

- ISG meeting on 3 December 2024 focused on the political context of the initiative, the call for evidence and the terms of reference for the impact assessment study. Written consultation was conducted from 3 December 2024 to 12 December 2024 on call for evidence and terms of reference for the impact assessment study.
- ISG meeting on 1 July 2025 focused on the first results of the call for evidence, and a first assessment of the policy options.
- ISG meeting on 3 December 2025 focused on updates regarding the legal base, the targeted consultation activities and the public consultation.
- ISG meeting on 15 April 2026 focused on a discussion of the Impact Assessment draft text. Written consultation was initiated on 13 April 2026 on the final draft of the impact assessment. Written feedback on the draft impact assessment was received by 17 April 2026.

www.parlament.gv.at

3. CONSULTATION OF THE RSB

An Upstream Meeting with the RSB has been held on 13 February 2026 and led to further refinement of the problem definition, notably by narrowing the scope and simplifying. The first version of the draft Impact Assessment report was submitted to the Regulatory Scrutiny Board (RSB) on 22 April 2026.

The RSB issued a positive opinion with comments, which were all implanted and had focussed on the following elements:

The IA report outlined the dynamic baseline by analysing the current situation of critical communication systems (CCS) in Member States, including planning and the current/planned interoperability. It specified which systems are currently in place e.g. narrowband, broadband, hybrid model in transition, and what plans and investment cycles there are to develop and/or upgrade existing systems in Member States.

The IA report was enriched with details regarding technological trends (e.g. direct-to-device satellite communication, encryption, etc.), the supply chain needs and related sovereignty aspects. The problem definition was enhanced in terms of the proportion of communications that presently suffer from interoperability shortcomings, cross border and within Member States.

The description of options, including the baseline, building on the Member States' level of preparedness and related plans was further explained. Key requirements following from the intervention, including minimum technical requirements were added and the report provides more details on the technical solutions and related uncertainties, trade-offs, key attributes of the new system (security, resilience, functionalities); and how it will be ensured that the requirements and technical solutions are future-proof, e.g. related to direct-to-device satellite communication.

The analysis was further detailed on the impacts of the proposed measures as well as potential unintended consequences. That concerned notably the assessment of costs and benefits accruing to all stakeholders and a clear overview on how the cost estimates from several Member States were extrapolated. The capital expenditures (CapEx) and operational expenditures (OpEx) for Mobile Network Operators (MNOs) were made clearer and quantified to the extent possible and it ws clarified that those costs are subject to renumeration and commercial agreements.

The sections analysing costs and benefits were further refined to outline benefits in terms of technological upgrades and facilitating data rich transfer are to be attributed to the EUCCS, or to other investments and developments. The costs and benefits were detailed, i.e. if indirect benefits to be taken into account and indirect costs to be factored in.

The report clarified further the very broad evidence basis on which EUCCS is founded, notably the underlying research projects, consultation with Member States, industry and other key stakeholders.

4. EVIDENCE, SOURCES AND QUALITY

For this impact assessment, the Commission collected data through various sources and consultations methods.

EUCCS is built in **close cooperation with European industry, therefore directly contributing to the overarching priorities of strategic autonomy and competitiveness**. European industry is partner in EUCCS Preparation and its precursor projects, with Airbus, Leonardo, Frequentis and Teltronic demonstrating the technical feasibility for EUCCS in ongoing trials with Member States.

www.parlament.gv.at

EUCCS has been presented at the most relevant international events relevant for critical communication in 2024 and 2025, including Critical Communication World (Dubai, Brussels), the Global Public Safety Operator Conference (Washington, Sydney) and the European Police Congress (Berlin). In compliance with the Better Regulation guidelines, DG HOME published the Call for Evidence in April 2025, and, in July 2025, contracted a nine-month-study to support the Impact Assessment. A CommissionOpen Public Consultation was conducted from 16 January until 10 April 2026 and targeted surveys as well as dedicated meetings have taken place with **representatives of industry**, such as providers of critical communication infrastructure and services and mobile network operators.

The research for the initiative and this impact assessment started with targeted surveys and interviews with EU Member States, which took place from July 2025 until June 2026 and mapped how Member States authorities are currently implementing their critical communications system.

The Commission conducted targeted surveys and interviews with critical communications industry representatives, as well as NGOs and other relevant associations, which took place from July 2025 until June 2026.

www.parlament.gv.at

ANNEX 2: STAKEHOLDER CONSULTATION (SYNOPSIS REPORT)

The Public Consultation was conducted between 16 January and 10 April 2026. The consultation aimed to gather evidence from a broad range of stakeholders on the key challenges, needs and expectations related to the functioning of critical communication systems across EU Member States, with particular attention to cross-border and inter-agency operational contexts.

In particular, the consultation sought to assess the extent to which existing systems enable effective cross-border and inter-agency communication, identify key operational, technical and governance-related challenges, and gather stakeholder feedback on possible policy approaches to enhance interoperability, resilience, security and coordination at EU level.

In total, 25 contributions were received, reflecting a broad range of perspectives across stakeholder groups and geographical contexts. Responses were collected through an online questionnaire (EU Survey) and included both closed questions, enabling quantitative analysis, and open-ended questions, providing qualitative insights. A more detailed breakdown indicates that public authorities constitute the largest group of respondents (52%, 13 out of 25), followed by EU citizens (20%, 5 out of 25) and companies (16%, 4 out of 25), with limited representation from business associations and trade unions.

From a geographical perspective, responses are concentrated in 5 Member States, with Germany accounting for the largest share (48%, 12 out of 25), followed by Spain (20%, 5 out of 25), Belgium (8%, 2 out of 25) and France (8%, 2 out of 25), and a limited number of contributions from the Netherlands.

All contributions were systematically reviewed and, where relevant analysed by stakeholder category and country of origin to identify recurring views, areas of convergence, and points of divergence. This approach allows for a nuanced understanding of stakeholder positions, including potential differences across institutional profiles and national contexts. While the consultation achieved broad outreach, the distribution of responses across stakeholder groups should be taken into account when interpreting the results, as certain categories, particularly public authorities, are more strongly represented.

Key findings

State of play

Stakeholder responses indicate a very strong consensus on the critical importance of reliable and secure cross-border and inter-agency communication for public authorities responsible for security and safety. A large majority of respondents consider such capabilities to be very important (88%, 22 out of 25), with only a marginal share indicating lower levels of importance. This highlights a near-unanimous recognition of the operational relevance of effective communication systems in an increasingly interconnected risk environment. At the same time, respondents consistently point to significant limitations in the current functioning of critical communication systems across Europe. A large majority consider that existing systems are not sufficient to support effective cross-border and inter-agency operations (76%, 19 out of 25). This suggests a clear gap between operational needs and current system performance, particularly in cross-border contexts.

This assessment is further corroborated by stakeholder views on the relevance of key problem drivers. Limited operational mobility and interoperability across borders and between agencies is identified as a major issue, with the vast majority of respondents considering it relevant or very relevant (84%, 21 out of 25). Similarly, limited resilience of critical communication infrastructure in the face of

www.parlament.gv.at

evolving threats is widely perceived as a significant problem (84%, 21 out of 25). Concerns related to limited autonomy and sovereignty of communication systems are also prominent, with 76% of respondents (19 out of 25) considering this issue relevant or very relevant.

The consultation also highlights a set of underlying structural factors contributing to these challenges. Limited interoperability due to heterogeneous technologies and varying levels of system maturity emerges as the most critical driver, as pointed out by 88% of respondents (22 out of 25). Similarly, fragmentation of governance frameworks, roles and procedures across agencies and MS is also identified as a key constraint (84%, 21 out of 25), alongside limitations in existing security standards and infrastructures (76%, 19 out of 25). In addition, a significant share of respondents points to dependencies on non-EU suppliers (68%, 17 out of 25), insufficient network coverage in certain areas (68%, 17 out of 25), and a fragmented EU market limiting innovation and standardisation (76%, 19 out of 25).

Corroborating quantitative data, qualitative feedback point to persistent technical and operational barriers, including the lack of cross-border compatibility of existing systems, the continued reliance on legacy narrowband technologies, and the complexity of replacing entrenched infrastructures. Respondents also highlight emerging risks related to cybersecurity vulnerabilities, dependence on third-country technologies, and insufficient spectrum availability. More broadly, stakeholders underline that fragmented and heterogeneous systems, combined with complex governance and regulatory environments, continue to hinder effective coordination and rapid response in cross-border emergency situations.

Overall, the consultation reveals a strong and consistent perception that, while the importance of mission-critical communications is widely acknowledged, current systems remain fragmented, insufficiently interoperable, and not fully adapted to evolving operational and security requirements.

Necessity and added value on EU intervention

Stakeholder responses indicate a strong perception that the identified challenges cannot be sufficiently addressed by Member States alone, and that EU-level intervention would be necessary to effectively tackle them. A very large majority of respondents consider EU action to needed (88%, 22 out of 25). Only a limited share expresses lower levels of necessity (12%, 3 out of 25), this suggests a broad recognition of the cross-border nature of the identified problems and the limitations of purely national approaches. While this overall assessment is widely shared, stakeholder differences emerge more clearly when considering market and regulatory aspects, with industry respondents expressing neutral views regarding the implications of EU intervention in terms of regulatory burden and flexibility, while public authorities and EU citizens more consistently emphasise the need for coordinated action to address cross-border operational challenges.

These findings are further reinforced by stakeholder views on the added value of EU action; indeed, respondents consistently attribute high significance to EU-level intervention across all assessed dimensions. Ensuring interoperability and operational mobility of public authorities across borders emerges as the area with the strongest perceived added value, with 96% of respondents (24 out of 25) considering it significant or very significant. Similarly, increasing the resilience and security of critical communication infrastructure is seen as highly dependent on EU action (88%, 22 out of 25).

Strong interest is also attributed to strengthening EU technological sovereignty and reducing dependencies on non-EU suppliers (80%, 20 out of 25 significant or very significant), as well as promoting technological innovation and competitiveness in the EU critical communication sector (88%, 22 out of 25). In this context, stakeholder views diverge more visibly on market implications, with industry respondents placing greater emphasis on potential impacts on investment conditions

www.parlament.gv.at

and flexibility, while EU citizens highlight opportunities for market integration, economies of scale and enhanced competitiveness.

Overall, these findings point to a strong convergence of views among stakeholders that EU-level action would provide substantial added value across multiple dimensions, particularly in addressing interoperability challenges, strengthening resilience and security, and supporting a more coordinated and integrated approach to critical communications across Europe.

Policy Options

Stakeholder responses reveal a differentiated perception of the suitability of the policy options, with clear patterns of convergence and some areas of more mixed views. The status quo option is widely perceived as inadequate, with a very large majority of respondents expressing disagreement (80%, 20 out of 25). The voluntary approach based on technical interconnectivity receives more mixed assessments. While a majority of respondents express disagreement (52%, 13 out of 25), a non-negligible share indicates support (20%, 5 out of 25), and a significant proportion remains neutral (24%, 6 out of 25).

By contrast, the option establishing a system of systems based on an EU legal framework is associated with a strong level of stakeholder support. A large majority of respondents express agreement (84%, 21 out of 25), including 44% (11 out of 25) who strongly agree, while only a limited share expresses disagreement (12%, 3 out of 25).

The option involving a fully centralised EU system receives comparatively more balanced assessments. While a majority of respondents express agreement (88%, 22 out of 25), a notable share expresses disagreement (28%, 7 out of 25).

Beyond the assessment of options, stakeholders emphasise a number of key considerations for the design of any potential EU intervention. In particular, a very large majority highlight the importance of ensuring clear roles and responsibilities across EU and national levels (92%, 23 out of 25), flexibility to adapt to technological change (92%, 23 out of 25), and proportionality and respect for Member State sovereignty (84%, 21 out of 25). Strong emphasis is also placed on ensuring coherence with existing EU legislation (88%, 22 out of 25), minimising administrative burden (76%, 19 out of 25), and carefully considering obligations for mobile network operators (68%, 17 out of 25).

Qualitative feedback further underlines the importance of addressing operational, legal and technical constraints, including the need for secure interoperability with legacy systems, alignment with EU security classification frameworks, standardisation of procedures, and access to funding for infrastructure deployment. Stakeholders also highlight concerns related to data protection, operational usability, and the need to balance EU-level coordination with national specificities and competencies.

Assessment of the impacts

These patterns are broadly reflected in the assessment of expected impacts. The status quo option is predominantly associated with negative impacts across economic, social and environmental dimensions, with negative or very negative ratings ranging from 60% (15 out of 25) for economic impacts to 64% (16 out of 25) for social impacts and 64% (16 out of 25) for environmental impacts. While this option is associated with relatively low or moderate adjustment and administrative costs (24%, 6 out of 25 indicating very low costs and 16%, 4 out of 25 neutral), respondents point to higher enforcement and opportunity costs, reflecting inefficiencies linked to the persistence of fragmented systems, which contributes to its overall negative impact profile.

www.parlament.gv.at

The voluntary interconnection option presents mixed opinions, with responses distributed across negative (40%, 10 out of 25) and positive (32%, 8 out of 25) economic impacts, and similar patterns across social and environmental dimensions, reflecting uncertainty regarding its overall effectiveness. This is mirrored in the cost assessment, where respondents identify moderate to high costs, particularly in terms of enforcement (32%, 8 out of 25 indicating high costs), suggesting that the coordination of voluntary arrangements may generate additional complexity without fully delivering the expected benefits. In this regard, stakeholder responses indicate that industry actors are more likely to perceive higher enforcement and opportunity costs linked to coordination burdens and the absence of harmonised frameworks, while public authorities tend to associate costs with inefficiencies arising from continued fragmentation rather than direct financial investment.

In contrast, the system of systems option is consistently associated with positive impacts, with 80% of respondents (20 out of 25) indicating positive or very positive economic impacts, 92% (23 out of 25) for social impacts, and 44% (11 out of 25) for environmental impacts, although the latter shows a more moderate distribution. These benefits are, however, associated with higher upfront costs, with a majority of respondents identifying high adjustment and compliance costs (48%, 12 out of 25), as well as high administrative (44%, 11 out of 25) and enforcement costs (40%, 10 out of 25). Differences across stakeholder groups are particularly visible in the perception of these costs, with industry respondents more frequently indicating high adjustment and enforcement costs due to direct exposure to implementation and infrastructure requirements, while public authorities tend to adopt a more balanced view, recognising both the scale of initial investments and the expected efficiency gains from reduced fragmentation. This suggests that, while the option entails significant initial investments, it is perceived as delivering more substantial and consistent benefits over time.

Finally, the centralised EU system option is generally associated with positive impacts, with 48% of respondents (12 out of 25) indicating positive or very positive economic impacts and 64% (16 out of 25) for both social and environmental impacts, although these are accompanied by a higher share of negative assessments compared to the system of systems. This more mixed perception is closely linked to the significantly higher cost expectations associated with this option, particularly in terms of very high adjustment and administrative costs (32%, 8 out of 25 and 36%, 9 out of 25 respectively), reflecting the scale and complexity of establishing a centralised infrastructure. Stakeholder responses indicate that industry actors are more likely to report very high adjustment and administrative costs, reflecting direct exposure to infrastructure deployment and compliance requirements, while public authorities also report high administrative costs linked to organisational restructuring and governance adaptation. EU citizens, although recognising the scale of upfront investments, more frequently emphasise the potential for long-term efficiency gains and reduced duplication across Member States.

Overall, the consultation reveals a clear preference for more coordinated approaches compared to the baseline and voluntary scenarios, while also highlighting important trade-offs in terms of costs, feasibility and governance that need to be considered in the design of EU-level intervention.

Conclusion

The analysis of the Public Consultation highlights a consistent recognition among stakeholders of the growing importance of critical communication systems in ensuring effective public safety, security and crisis response across Europe. At the same time, the findings point to persistent limitations in the current functioning of these systems, especially when approaching cross-border and inter-agency contexts. Fragmentation of technologies, governance frameworks and operational procedures continue to constrain interoperability, limit operational mobility and reduce the overall effectiveness of coordinated responses to emergencies and security incidents.

www.parlament.gv.at

These challenges are perceived as structural in nature and closely linked to the evolving operational and threat environment. In this context, the current landscape is not considered fully adequate to support the needs of public authorities responsible for security and safety.

The consultation confirms the overall perception that these issues cannot be effectively addressed through isolated national actions. The cross-border dimension of critical communications, combined with the need for common standards, shared procedures and enhanced resilience, points to the need for more coordinated approaches at EU level. The role of EU intervention in enabling interoperability, strengthening security and resilience, supporting technological innovation, and fostering a more integrated and predictable framework is widely expected among the various stakeholders.

At the same time, the assessment of policy options highlights the relevance of balancing the benefits of increased coordination with considerations related to feasibility, costs and governance. Structured and coordinated approaches are generally seen as better suited to addressing the identified challenges, however, stakeholders emphasise the need to preserve flexibility, respect Member State competencies, and ensure that any future framework remains adaptable to national specificities and operational realities.

Overall, the consultation results point to a clear need to address existing gaps in interoperability, resilience and coordination, while highlighting the importance of designing solutions that are both effective at EU level and workable in practice. This requires a calibrated approach that combines common principles and standards with sufficient flexibility to accommodate the diversity of systems and operational contexts across Europe.

www.parlament.gv.at

ANNEX 3: WHO IS AFFECTED AND HOW?

1. PRACTICAL IMPLICATIONS OF THE INITIATIVE

5 million emergency services across Europe will benefit from inter-agency and cross-border critical communications enabling faster and more efficient response to incidents and major crises. Citizens across Europe will benefit from reduced response time of emergency services in case of accidents, security incidents, and natural disasters. There will be positive impacts for providers of critical infrastructure services and solutions. Mobile network operators will have to make arrangements to facilitate critical communications on commercial networks.

2. SUMMARY OF COSTS AND BENEFITS

I. Overview of Benefits (total for all provisions) – Preferred Option		
Description	*Amount*	*Comments*
Direct benefits		
Enhanced cooperation and information exchange for emergency services	5 million users in 31 Member States interconnected via EUCCS	Faster and more efficient response to in case of accidents, security incidents, and natural disasters
Strengthening of EU security industry to provide state of the art critical communications technology	Close to 14 billion EUR investments to be made at the EU and Member States level combined, to be carried out in harmonised timelines by 2030, 2033 and 2036	Providers of critical communications infrastructure, solutions and services will directly benefit from streamlined investments from the EU and Member States in mission critical broadband, creating business opportunities and enhancing European competitiveness at the international level
Indirect benefits		
Strengthening of EU strategic autonomy in the critical communications sector	Up to 9000 European companies could benefit from a dynamic investment ecosystem created under EUCCS	EUCCS will enhance strategic autonomy and give them a competitive advantage to the European industry also beyond Europe

(1) Estimates are gross values relative to the baseline for the preferred option as a whole (i.e. the impact of individual actions/obligations of the preferred option are aggregated together); (2) Please indicate in the comments column which stakeholder group is the main recipient of the benefit;(3) For reductions in regulatory costs, please describe in the comments column the details as to how the saving arises (e.g. reductions in adjustment costs, administrative costs, regulatory charges, enforcement costs, etc.;);.

II. Overview of costs – Preferred option							
		Citizens/Consumers		**Businesses**		**Administrations**	
		One-off	**Recurrent**	**One-off**	**Recurrent**	**One-off**	**Recurrent**
Policy Option 2.1	Direct adjustment costs	N/A	N/A	N/A	N/A	€ 794,919,480.98	€ 2,478,045,299.38
	Direct administrative costs	N/A	N/A	N/A	N/A	€ 189,624,205.24	€ 108,808,668.70
	Direct regulatory fees and charges	N/A	N/A	N/A	N/A	N/A	N/A
	Direct enforcement costs	N/A	N/A	N/A	N/A	N/A	N/A

www.parlament.gv.at

	Indirect costs	N/A	N/A	N/A	N/A		

(1) Estimates (gross values) to be provided with respect to the baseline; (2) costs are provided for each identifiable action/obligation of the preferred option otherwise for all retained options when no preferred option is specified; (3) If relevant and available, please present information on costs according to the standard typology of costs (adjustment costs, administrative costs, regulatory charges, enforcement costs, indirect costs;).

III. Application of the 'one in, one out' approach – Preferred option(s)			
[M€]	**One-off** (annualised total net present value over the relevant period)	**Recurrent** (nominal values per year)	**Total**
Businesses			
New administrative burdens (INs)	N/A	N/A	N/A
Removed administrative burdens (OUTs)	N/A	N/A	N/A
Net administrative burdens*	N/A	N/A	N/A
Adjustment costs**	NA	N/A	
Citizens			
New administrative burdens (INs)	N/A	N/A	N/A
Removed administrative burdens (OUTs)	N/A	N/A	N/A
Net administrative burdens*	N/A	N/A	N/A
Adjustment costs**	N/A	N/A	
Total administrative burdens* **	**N/A**	**N/A**	**N/A**

(*) Net administrative burdens = INs – OUTs;
(**) Adjustment costs falling under the scope of the OIOO approach are the same as reported in Table 2 above. Non-annualised values;
(***) Total administrative burdens = Net administrative burdens for businesses + net administrative burdens for citizens.

3. RELEVANT SUSTAINABLE DEVELOPMENT GOALS

IV. Overview of relevant Sustainable Development Goals – Preferred Option(s)		
Relevant SDG	**Expected progress towards the Goal**	**Comments**
SDG no. 16 – Promote peaceful and inclusive societies for sustainable development, provide access to justice for all, and build effective, accountable, and inclusive institutions at all levels	By enabling interoperable, secure, and resilient cross-border communication among public authorities responsible for security and safety, the EUCCS strengthens the operational capacity of these institutions, supports efficient coordination in crisis situations, and enhances the accountability and reliability of public security and safety services.	

www.parlament.gv.at

SDG no. 11 - Make cities and human settlements inclusive, safe, resilient and sustainable	By 2030, significantly reduce the number of deaths and the number of people affected and substantially decrease the direct economic losses relative to global gross domestic product caused by disasters, including water-related disasters, with a focus on protecting the poor and people in vulnerable situations.	
SDG no. 13 - Strengthen resilience and adaptive capacity to climate-related hazards and natural disasters in all countries	The EUCCS will strengthen resilience and adaptive capacity to climate-related hazards and natural disasters in all countries.	
SDG no. 16 - Promote peaceful and inclusive societies for sustainable development, provide access to justice for all and build effective, accountable and inclusive institutions at all levels	The EUCCS will Strengthen relevant national institutions, including through international cooperation, for building capacity at all levels to prevent violence and combat terrorism and crime.	

ANNEX 4: ANALYTICAL METHODS

The stakeholder consultation activities carried out under this Study aimed to support the impact assessment on the EUCCS initiative by collecting evidence on the current state of critical communication systems across Europe, the main challenges affecting cross-border mission-critical communications, stakeholders' views on the policy options under consideration for the establishment of the EUCCS, and their economic, social, environmental, and technical impacts.

In line with the Better Regulation Guidelines, the consultations were designed to ensure that the impact assessment is grounded in evidence from the stakeholders most directly concerned by the initiative.

The Call for Evidence feedback was qualitatively analysed by recognising stakeholder positions, recurring issues in cross-border critical communications, as well as preferences regarding the policy options identified for the establishment of the EUCCS.

The Public Consultation was designed to engage a broad spectrum of public and private stakeholders and collect both quantitative and qualitative evidence on the needs, challenges and expectations related to cross-border mission-critical communication in Europe. Contributions received through the questionnaire were reviewed and analysed as a whole and, where relevant, by stakeholder category in order to identify recurring views, areas of convergence and points of divergence.

The targeted survey for EU Member States public authorities collected both quantitative and qualitative information on the governance of critical communications, existing and planned technical capabilities in the EU Member States, interoperability, resilience, cross-border use cases, perceived challenges and the expected impacts of the policy options for the establishment of the EUCCS. 27 replies were received in total, corresponding to 25 countries. For analytical purposes, duplicate responses from France and Sweden were consolidated to a unique country-based response.

The targeted survey for industry representatives collected mainly qualitative information on the current state of the market, technical and operational challenges, and views on the policy options and their impacts. The survey covered organisations identifying as 3GPP/mission critical technology providers, TETRA technology providers, critical communications device providers, and Mobile Network Operators.

The exploratory and targeted interviews were semi-structured and organised around tailored interview guides depending on the stakeholder group. Interview minutes were shared with the interviewees for review and validation. Inputs from EU institutions and agencies, international organisations, end-users, industry representatives, and Mission Critical Communication Group working group leaders were analysed qualitatively to identify recurring themes, converging views and points of divergence across stakeholder groups. Conversely, interviews targeting European authorities collected quantitative data on the costs of the policy options for the establishment of the EUCCS and were therefore analysed using quantitative methods.

The co-creation workshops were organised to support the development and validation of the intervention logic and policy measures for the establishment of the EUCCS. Bringing together representatives from EU institutions and agencies, European public authorities, and end-user organisations, these workshops applied design thinking principles to test preliminary hypotheses and foster a shared understanding of the problems, problem drivers, external factors, general and specific objectives, policy options, and expected impacts. The discussions and outputs from these workshops

www.parlament.gv.at

were reviewed qualitatively and used to refine the analytical framework and inform the subsequent steps of the Study.

Finally, the Mission Critical Communication Group meetings were used as an additional consultation channel to collect expert input from European public authorities, as well as EU bodies and agencies. Inputs gathered through these meetings were used to complement and contextualise the evidence collected through the other consultation activities.

For all consultation activities, the data were cleaned and analysed using both descriptive and qualitative methods. Quantitative findings were aggregated in tables and charts using spreadsheets, while open-text responses and interview minutes were reviewed to identify common themes, explanatory factors and illustrative stakeholder positions. The results from the different consultation channels were compared to identify points of convergence and divergence.

The primary evidence stems extensive consultation of Member States and their emergency services. That was achieved via a series of surveys and targeted interview conducted by the contractor team that delivered the supporting study, as well as direct outreach and additional questionnaires of DG HOME to the Mission Critical Communication Group, which comprises almost all competent authorities of Member States. More specifically:

- Call for Evidence (April 2025 - May 2025), with 24 responses from EU citizens - companies - public authorities - public agencies - industry and interest associations - NGOs, to obtain feedback on the Commission's understanding of the problem and possible solutions and give us any relevant information that they may have, including on possible impacts of the different options.

- Public Consultation (January 2026 – April 2026), with 25 responses from EU citizens – business associations - public authorities – companies – trade unions – NGOs, to engage a broad spectrum of public and private stakeholders to gather relevant information on the needs, challenges, and expectations related to cross-border mission-critical communication.

- Targeted survey for EU Member States public authorities (November 2025 – January 2026), with 25 responses, to identify the state-of-play of critical communication systems at the national level, gather information on the needs for EU intervention and cross-border communications, and collect views on the policy options for the EUCCS, as well as their impacts and cost estimates.

- Targeted survey for industry representatives (November 2025 – December 2025), with 9 responses, to identify the current state of critical communications systems from the industry perspective, gather information on the needs for EU intervention and cross-border communication, and collect views on the policy options for the EUCCS, including their impacts and cost estimates.

- 14 exploratory interviews (September 2025) with EU institutions and agencies - EU MS public authorities - industry representatives - end-users - international organisations, to gain a deeper understanding of the political context, identify potential challenges and limitations, draw lessons from related EU-funded projects, and gather preliminary feedback on the current issues, the rationale for the EUCCS, and its objectives and drivers.

- 21 targeted interviews (January 2026 – March 2026) with EU MS public authorities - industry representatives - end-users of critical communication systems – leaders of the Mission Critical

www.parlament.gv.at

Communication Group (MCCG) working groups, to collect views from underrepresented stakeholder groups, clarify any gaps or uncertainties from the surveys and gather quantitative data for the impact assessment.

- 3 co-creation workshops (2 October 2025, 24 October 2025 and 19 November 2025) with EU institutions and agencies - EU MS public authorities - end-user organisation, to reach a common agreement and alignment among all participants on the intervention logic (problems, problem drivers, external factors, general and specific objectives, policy options and expected impacts) and the policy measures for the EUCCS.

- Consultations of the MCCG during 3 meetings (22-23 October 2025, 11 December 2025 and 26 February 2026), to collect the expert group's opinions and ask targeted questions to gather quantitative and qualitative data.

Consultation session (10 March 2026) with Mobile Network Operators (MNOs) representative organisations (Global System for Mobile Communications Association (GSMA), The Critical Communications Association (TCCA) and Public Safety Communication Europe (PSCE Europe)), to gather information on the needs for EU intervention and cross-border communication, and collect views on the policy options for the EUCCS, including their impacts and cost estimates, with a particular focus on MNOs.The table below summarises the consultation activities carried out, indicating for each consultation type its period, number of consultations, objectives, stakeholder groups covered, and number of respondents.

www.parlament.gv.at

Consultation activity	Period	Number of consultations	Objectives	Stakeholder groups covered	Number of respondents
Call for Evidence analysis	Sept-Oct 2025	1	Analyse the feedback received on the Call for evidence published on the 'Have Your Say' web portal.	• EU citizens (6) • Companies (5) • Public authorities (4) • Public agencies (3) • Industry and interest associations (3) • Non-governmental organisations (NGOs) (3)	24
Public Consultation	Jan-Apr 2026	1	Engage a broad spectrum of public and private stakeholders to gather relevant information on the needs, challenges, and expectations related to cross-border mission-critical communication in EU MS and SAC.	• EU citizens (5) • EU MS and SAC public authorities (13) • Business associations (1) • Companies (4) • Trade Unions (1) • NGOs (1)	25
Targeted survey for EU MS and SAC	Nov 2025-Jan 2026	1	Identify the state-of-play of critical communication systems at the national level, gather information on the needs for EU intervention and cross-border communications, and collect views on the policy options for the EUCCS, as well as their impacts and cost estimates.	• EU MS and SAC public authorities	25
Targeted survey for industry representatives	Nov-Dec 2025	1	Identify the current state of critical communications systems from the industry perspective, gather information on the needs for EU intervention and cross-border communication, and collect views on the policy options for the EUCCS, including their impacts and cost estimates.	• Industry representatives (critical communication system providers, MNOs)	9

www.parlament.gv.at

Consultation activity	Period	Number of consultations	Objectives	Stakeholder groups covered	Number of respondents
Exploratory interviews	Sept 2025	14	Gain a deeper understanding of the political context, identify potential challenges and limitations, draw lessons from related EU-funded projects, and gather preliminary feedback on the current issues, the rationale for the EUCCS, and its objectives and drivers.	• EU institutions and agencies (6) • EU MS and SAC public authorities (3) • Industry representatives (3) • End-users (1) • International organisations (1)	14
Targeted interviews	Jan-Mar 2026	21	Collect views from underrepresented stakeholder groups, clarify any gaps or uncertainties from the surveys and gather quantitative data for the impact assessment.	• EU MS and SAC public authorities (9) • Industry representatives (3) • End-users of critical communication systems (2) • MCCG working group leaders (7)	21
Co-creation workshops	02 Oct 2025 24 Oct 2025 19 Nov 2025	3	Reach a common agreement and alignment among all participants on the intervention logic (problems, problem drivers, external factors, general and specific objectives, policy options and expected impacts) and the policy measures for the EUCCS.	• EU institutions and agencies • EU MS and SAC public authorities • End-user organisations	/
MCCG meetings	22-23 Oct 2025 11 Dec 2025 26 Feb 2026	3	Collect the expert group's opinions and ask targeted questions to gather quantitative and qualitative data.	• EU MS and SAC public authorities • EU institutions and agencies	/

www.parlament.gv.at

ANNEX 5: COMPETITIVENESS CHECK

1. Overview of impacts on competitiveness

Dimensions of Competitiveness	**Impact of the initiative (++ / + / 0 / - / -- / n.a.)**	**References to sub-sections of the main report or annexes**
Cost and price competitiveness	++	Technical impact analysis
International competitiveness	++	Technical impact analysis
Capacity to innovate	++	Technical impact analysis
SME competitiveness	++	Annex 6

2. Synthetic assessment

EUCCS is expected to have a positive impact on European competitiveness in the critical communication domain. Critical communication is a small but very specialised segment of the overall telecommunication sector and European companies are currently among the leading providers and exporters of services, specifically in the narrowband technologies. The establishment of EUCCS will support the business opportunities by providing harmonised and predictable timeline for the deployment of mission critical broadband in Member States. Specialised industry can thus adapt and offer tailored services and solutions, benefiting from procurement launched by Member States and increased demand for new devices, services and solutions that facilitate broadband-based functionalities for emergency services.

The move to a 3GPP based EUCCS with the de-coupling of the three key elements (below) of the CCS supplier offerings will result in increased competitiveness in each domain.

i. user equipment (UE)
ii. radio-access and transport network
iii. the central mission critical servers

Specifically, the migration to ubiquitous mobile phone networks will result in opening to competition of the EU market. Basing EU on mobile phone technologies will create a much larger potential supplier base, moving the supply chain to outside of the niche market occupied by the TETRA and TETRAPOL suppliers.

Similarly, the mission critical market will be de-coupled from the radio-access networks and will connect to the UE in the same fashion as mobile phone apps do with mobile services. This opens the ecosystem to value-add services that can be offered over the CCS network by new entrants with much lower barriers to entry, creating a more competitive ecosystem and driving prices lower as a result. Given the number of National Authorities and range of nations that would be covered by the EUCCS, this would create a very unique market that could support a multitude of offerings from smaller companies.

Competition for the mobile phone contracts to support the Public Protection and Disaster Relief users, while only small in numbers in absolute terms, constitute a very large single contract for mobile phone companies. This should create price and functionality competition amongst mobile service providers.

Formation of EUCCS will drive the evolution of critical communication broadband market worldwide. Europe is readily leading in multi-agency communication via national shared public safety narrowband networks. European based TETRA and Digital Mobile Radio (DMR) technologies are globally dominant in the digital narrowband sector outside North America. With 3GPP based Broadband transition fundamentally 5G based solutions will be deployed throughout the world. To function properly EUCCS must address many challenges other nations will be facing as their broadband transition commences. By addressing the challenges like broadband interoperability best practises and standards are set others will de facto follow giving an edge to EUCCS suppliers.

3. Competitive position of the most affected sectors

General market including consumers

3GPP UE sector: this is not a sector where the EU has any meaningful presence.

3GPP mobile networks: the EU has a large presence here, but it is unlikely to be affected one way or another by the EUCCS.

3GPP mission critical services: this is a sector where the EU has an important presence which would benefit from the increased innovation and competition of a 3GPP EUCCS. Conversely, Remaining on TETRA and TETRAPOL based systems would dilute commercial incentives for the existing suppliers to invest in 3GPP based solutions that would be marketable globally.

Critical Communications market sectors

Devices

- Chipset: dependency on Qualcomm and Mediatek
- Operating system: currently dependency on Android and iOS, opportunity to build independent OS ecosystem
- Design: several sector specific leading companies
- Assembly: full competence – competitive if supply chain security is an important factor

Networks

- Core and RAN: Europe is leading 3GPP based defence development that has significant synergies with critical communication sector.
- EUCCS via the national Public Protection and Disaster Relief BB networks drives availability, resiliency, reliability and security demand in general in mobile networks. This has already generated many new business opportunities in network design, management, monitoring, automation. These innovations will be required not only for Public Protection and Disaster Relief Broadband services, but also for consumer and enterprise services as recognition of society mobile communication dependency increases.

www.parlament.gv.at

Applications

- European challenge is very fragmented market requiring plenty of localisation among others due to different languages leading many times to project instead of product type implementations. EUCCS opportunity is to foster more common baseline requirements leading to greater market, yet localised products that can be adjusted to target markets outside Europe.
- European benefit is very advanced multi-agency and partly multi-national co-operation that has driven efficient operational models and products supporting them. These field operational models can be exported to other nations with the product and services support. EUCCS will drive this development cross national borders

Society perspective

- Societies are deeply dependent on always functioning mobile communication. EUCCS increases the general European service availability to all citizens and enterprises as EUCCS related investments in hardening, power resilience etc. largely impacts commercial networks.

www.parlament.gv.at

ANNEX 6: SME CHECK

OVERVIEW OF IMPACTS ON SMES

Relevance for SMEs
Based on SME filter and the ISG discussion, this initiative is relevant for SMEs[96].
(1) IDENTIFICATION OF AFFECTED BUSINESSES AND ASSESSMENT OF RELEVANCE
Are SMEs directly affected? In which sectors?
Yes. Providers of: - critical communication services, infrastructure and equipment. - mobile and control room and testing applications. - integrators of multi-sensor systems for situational awareness - providers of integrated deployable communication systems - threat intelligence and vulnerability assessment security services
Estimated number of directly affected SMEs
We estimate 9,000 SMEs are offered new market opportunities. For example: 15% 1.350 Critical communication services, infrastructure and equipment. 35% 3.150 Mobile and control room and testing applications. 14% 1.260 Integrators of multi-sensor systems for situational awareness 15% 1.350 Providers of integrated deployable communication systems 10% 900 Threat intelligence and vulnerability assessment security services 1% 50 Training Services 10% 900 Specific consulting, for example where national competent authorities 100% 9.000 Those providing existing Applications will be encouraged to become compatible with EUCCS, which is not considered to be a complex process.
Estimated number of employees in directly affected SMEs
Over 450 000
Are SMEs indirectly affected? *(No)* **In which sectors? What is the estimated number of indirectly affected SMEs and employees?**

[96] https://ec.europa.eu/docsroom/documents/63274

www.parlament.gv.at

Yes. Most society sectors will benefit from higher availability, resilience, improved mobile network coverage - especially in rural areas. Better reliable communication improves rural areas companies – typically SMEs – competitivity as they can better offer their services utilising digitalised channels.
(2) CONSULTATION OF SME STAKEHOLDERS
How has the input from the SME community been taken into consideration?
Yes, SMEs participated in the Call for Evidence, the Commission Open Public Consultation and the targeted stakeholders' consolations. Furthermore, SME are part of the consortia that developed the technical basis for EUCCS, including the current ISF-funded EUCCS Preparation Project. In BroadWay and EUCCS Preparation, ~10 SMEs were directly involved in the process, and ~50 involved in outside engagements.
Are SMEs' views different from those of large businesses?
The Call for Evidence, the Commission Open Public Consultation, the active integration in the EUCCS Preparation Project as well as the targeted stakeholder consultations have not shown any difference between the position of SME and bigger players in the market. The large businesses contracted for the technical work under the EU-funded EUCCS Preparation project have all engaged with SME's who have developed the core functionality of Mission Critical Services.
(3) ASSESSMENT OF IMPACTS ON SMEs[97]
What are the estimated direct costs for SMEs of the preferred policy option? There are no costs for SME related to the preferred policy option.
Qualitative assessment
N/A
Quantitative assessment
N/A
What are the estimated direct benefits/cost savings for SMEs of the preferred policy option[98]?
Qualitative assessment
Providers of critical communication services, infrastructure and equipment, integrated systems and applications are in many cases SME. They will benefit from the establishment of EUCCS, given it provides clear timelines and incentives for the modernisation of critical communication systems in Member States. That creates in turn business opportunities as new services and devices will be required by emergency services. Especially for services, devices and applications there is big

[97] The costs and benefits data in this annex are consistent with the data in annex 3. The preferred option includes the mitigating measures listed in section 4.
[98] The direct benefits for SMEs can also be cost savings.

www.parlament.gv.at

potential for smaller industry players and start-ups, while on the infrastructure side traditionally bigger enterprises define the market. This is already seen through EUCCS Preparation, as explained above.
Quantitative assessment
The global market for Applications (see point 1) alone, is $11.2 billion by 2030 (quoted in the SNS Telecom Public Safety Market report 2026[99]). Scaled to Europe (15%) is ~€1.65 billion. This covers the following which are mostly provided by SMEs, or large industry working with SMEs: • Mission-Critical Voice & Group Communications • Real-Time Video Transmission • Messaging, File Transfer & Presence Services • Mobile Office & Field Applications • Location Services & Mapping • Situational Awareness • Command & Control • AR/VR/MR (Augmented, Virtual & Mixed Reality) Integration of systems (2 bullets in point 1) has a global market of $5.2 billion with a scaled estimate for Europe of €0.8 billion. A market opportunity for SMEs of ~€2.45 billion. Considering 9000 SMEs, there would be ~€27M opportunity each.
What are the indirect impacts of this initiative on SMEs? N/A
(4) MINIMISING NEGATIVE IMPACTS ON SMES
Are SMEs disproportionately affected compared to large companies?
No.
If yes, are there any specific subgroups of SMEs more exposed than others?
N/A
Have mitigating measures been included in the preferred option/proposal?
No
CONTRIBUTION TO THE 35% BURDEN REDUCTION TARGET FOR SMES

[99] Public Safety LTE & 5G Market: 2025-2030: Opportunties, Challenges, Strategies and Forecasts https://www.snstelecom.com/public-safety-lte

www.parlament.gv.at

Are there any administrative cost savings relevant for the 35% burden reduction target for SMEs?
No.

www.parlament.gv.at

ANNEX 7: ADDITIONAL MATERIALS

7.1 Graphs supporting this Impact Assessment

Below are graphs and visualizations that help better substantiate the claims made throughout the report and offer evidence. All figures are referenced to in footnotes throughout the text for ease of consultation.

Figure 1. Rise in the number of activations of the UCPM mechanism

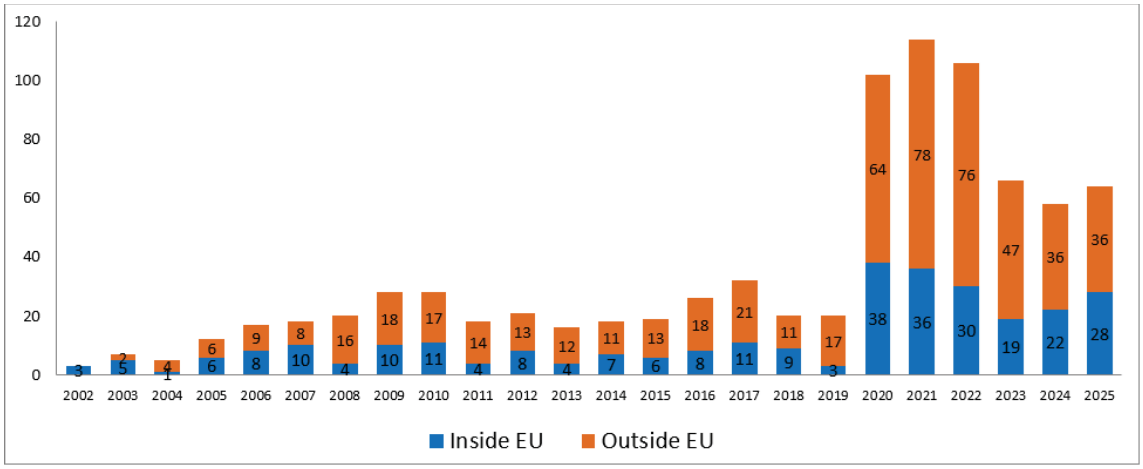


Figure 2. Maturity level of national critical communication systems in Member States

Narrowband system (MS)	Narrowband system (SAC)	Hybrid configurations (MS)	Hybrid configurations (SAC)
12	NO	11	1

Figure 3. Expected entry into EUCCS (data collected during the 12th MCCG Meeting, 22-23 April 2026)

2030	2033	2036
11	4	15

www.parlament.gv.at

Figure 4. Reported level of interoperability with CCS in other MS and SAC

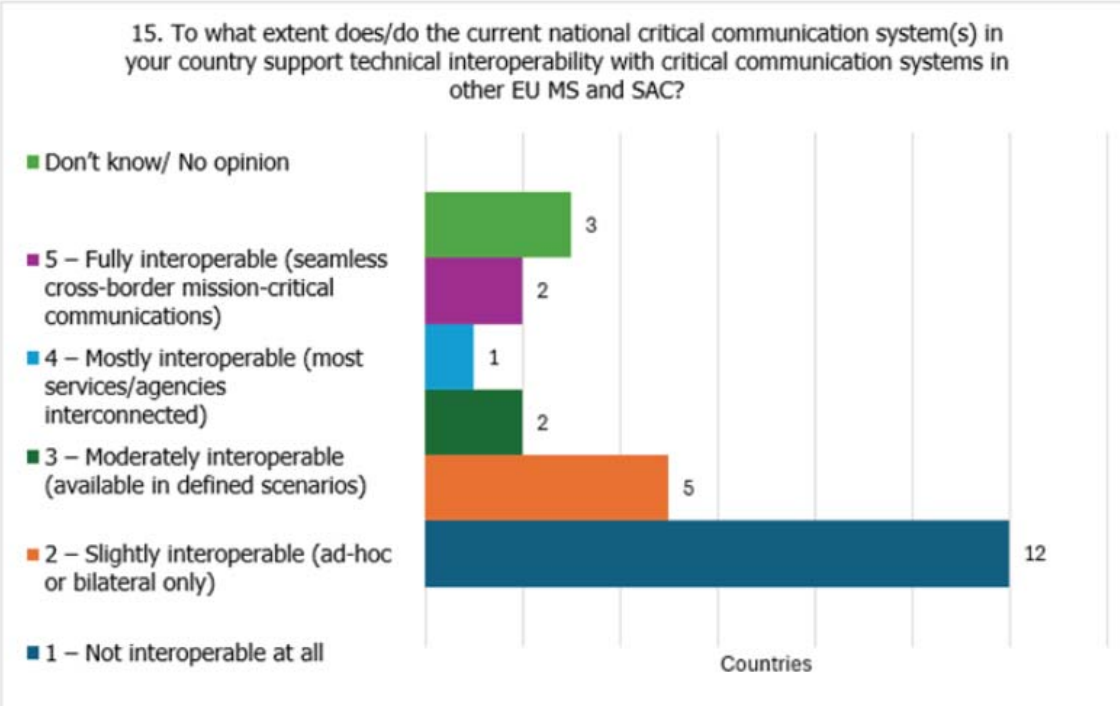
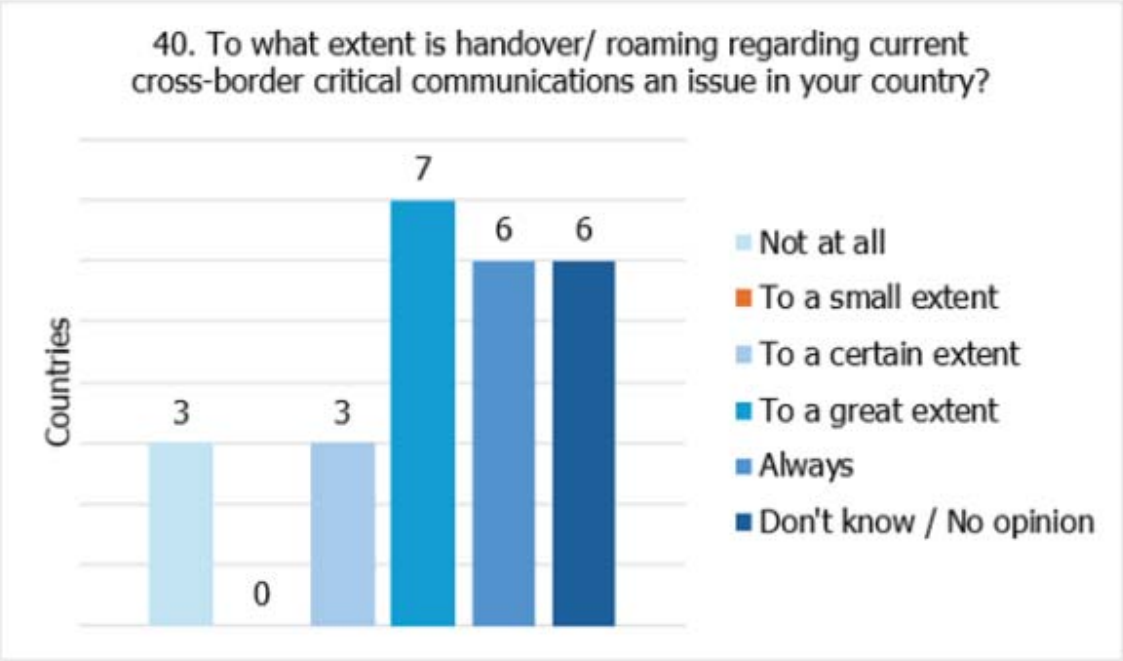


Figure 5. Reported level of handover/roaming being an issue in cross-border critical communications



www.parlament.gv.at

Figure 6. Reported resilience of national critical communication systems in the EU Member States[100]

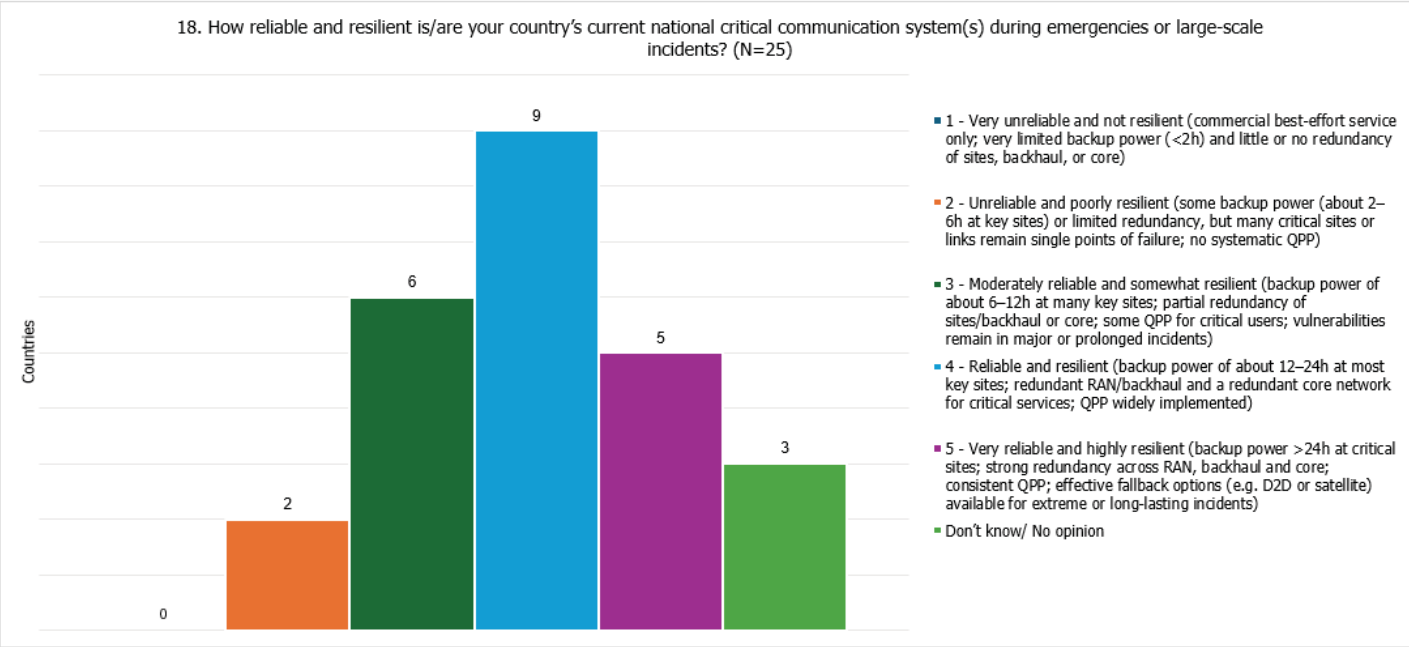


Figure 7. Reported period since national critical communications systems became operational in the MS

---

[100] The categories of reliability and resilience in the targeted survey are defined as follows:
1 - Very unreliable and not resilient (commercial best-effort service only; very limited backup power (<2h) and little or no redundancy of sites, backhaul, or core);
2 - Unreliable and poorly resilient (some backup power (about 2–6h at key sites) or limited redundancy, but many critical sites or links remain single points of failure; no systematic QPP);
3 - Moderately reliable and somewhat resilient (backup power of about 6–12h at many key sites; partial redundancy of sites/backhaul or core; some QPP for critical users; vulnerabilities remain in major or prolonged incidents);
4 - Reliable and resilient (backup power of about 12–24h at most key sites; redundant RAN/backhaul and a redundant core network for critical services; QPP widely implemented);
5 - Very reliable and highly resilient (backup power >24h at critical sites; strong redundancy across RAN, backhaul and core; consistent QPP; effective fallback options (e.g. D2D or satellite) available for extreme or long-lasting incidents).

www.parlament.gv.at

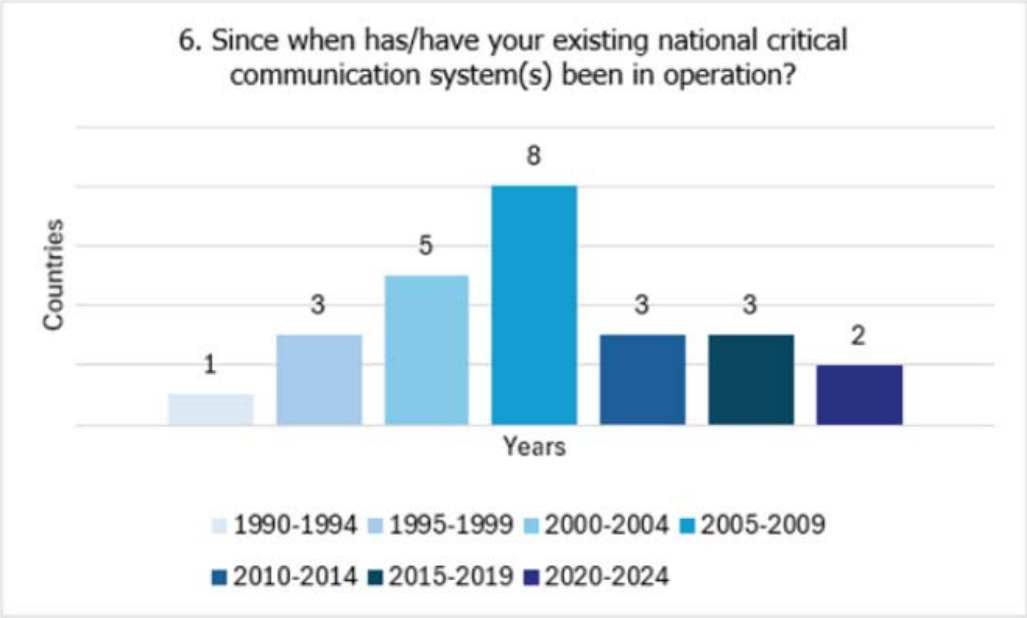
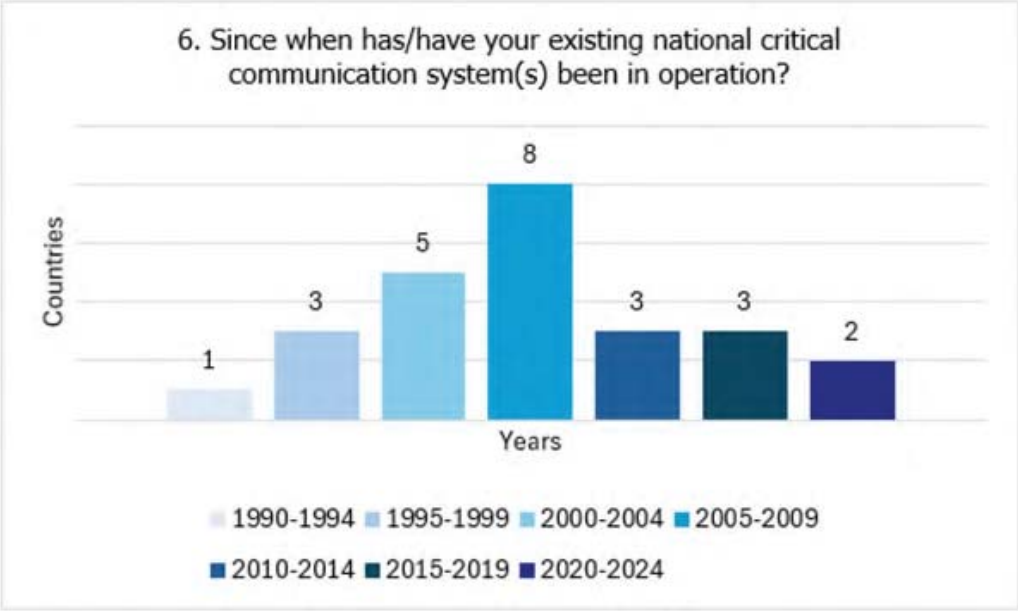


Figure 8. Reported period since national critical communications systems became operational in the MS



www.parlament.gv.at

Figure 9. Reported coverage of national critical communication systems in EU Member States

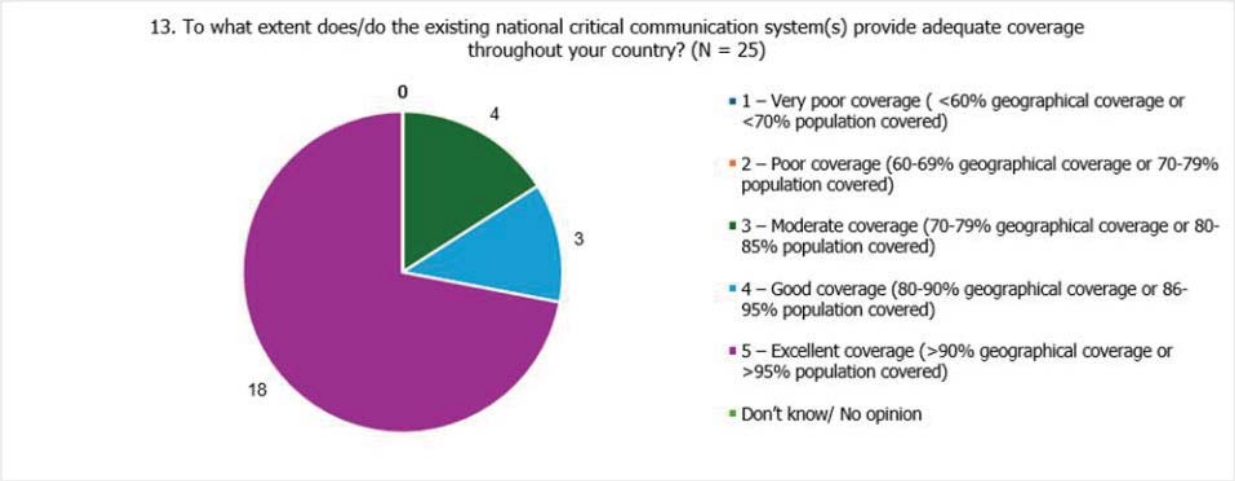
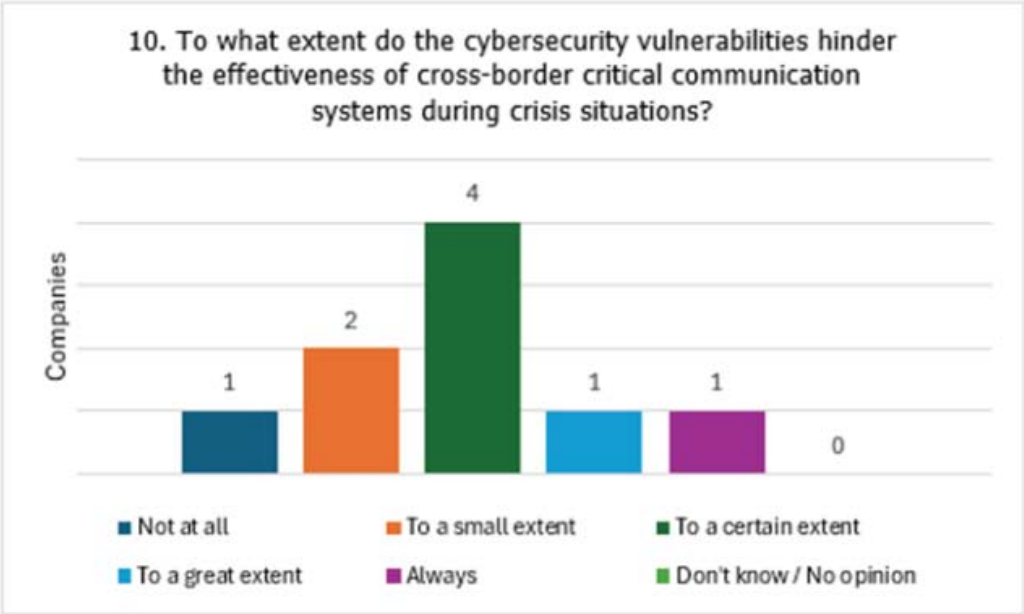


Figure 10. Reported impact of cybersecurity vulnerabilities on the effectiveness of cross-border operations across MS



www.parlament.gv.at

Figure 11. Reported impact of the absence of backup systems on the effectiveness of cross-border operations across EU MS and SAC

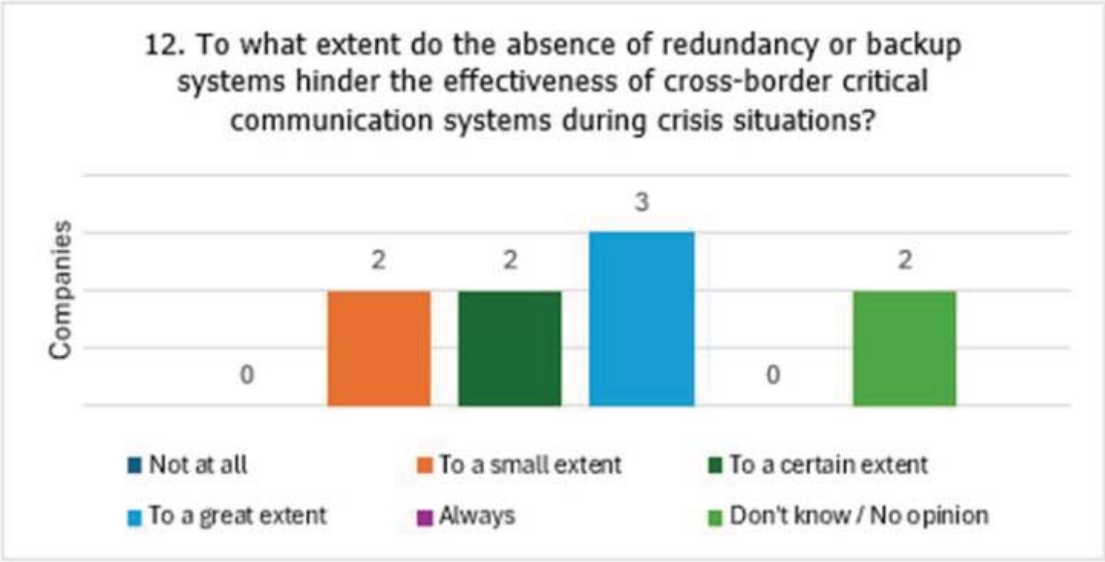
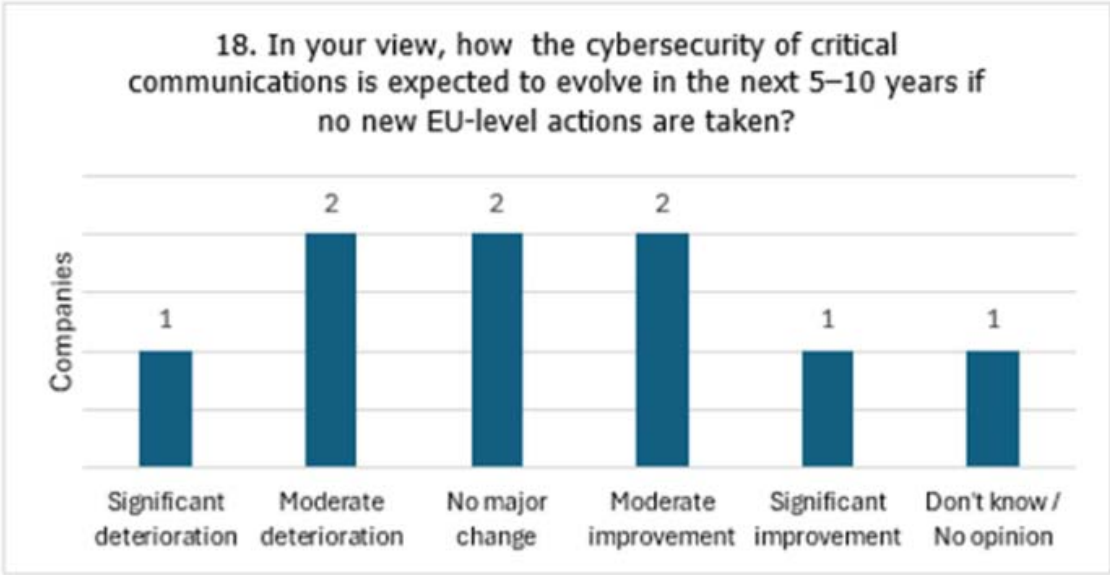


Figure 12. Reported cybersecurity evolution of critical communication systems in the next 5-10 years in the scenario of no EU action



www.parlament.gv.at

Figure 13. Reported level of seamless Public Protection and Disaster Relief roaming across borders in MS

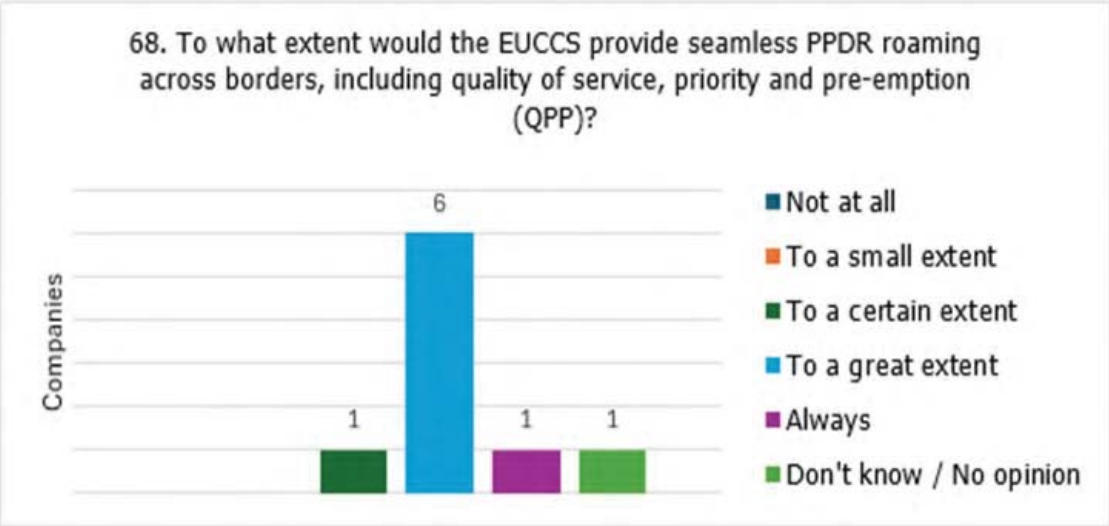
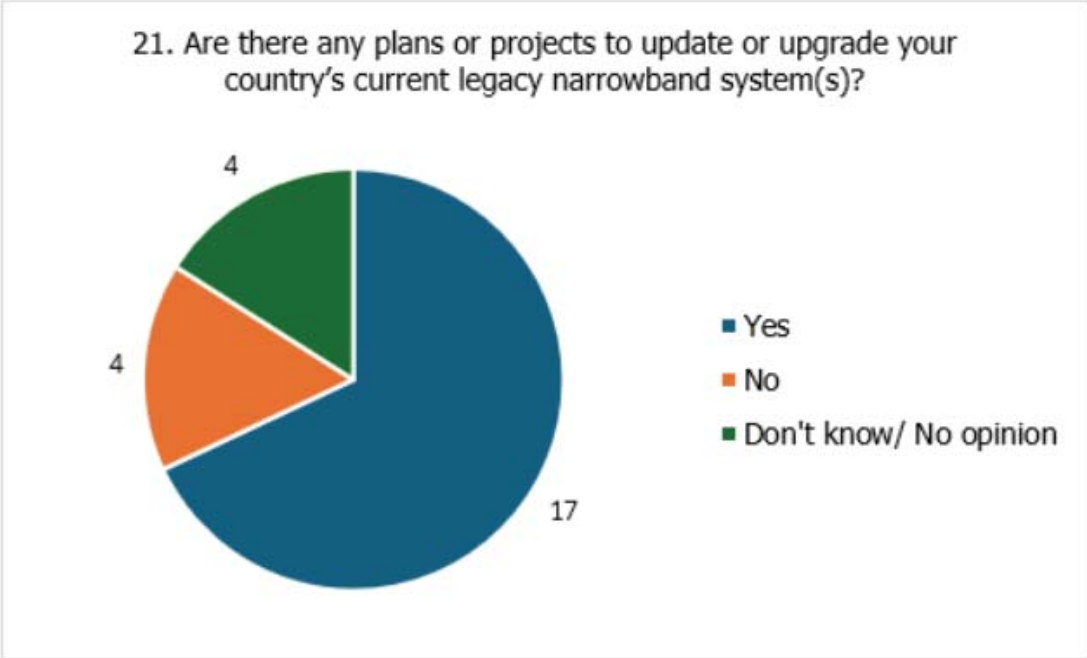
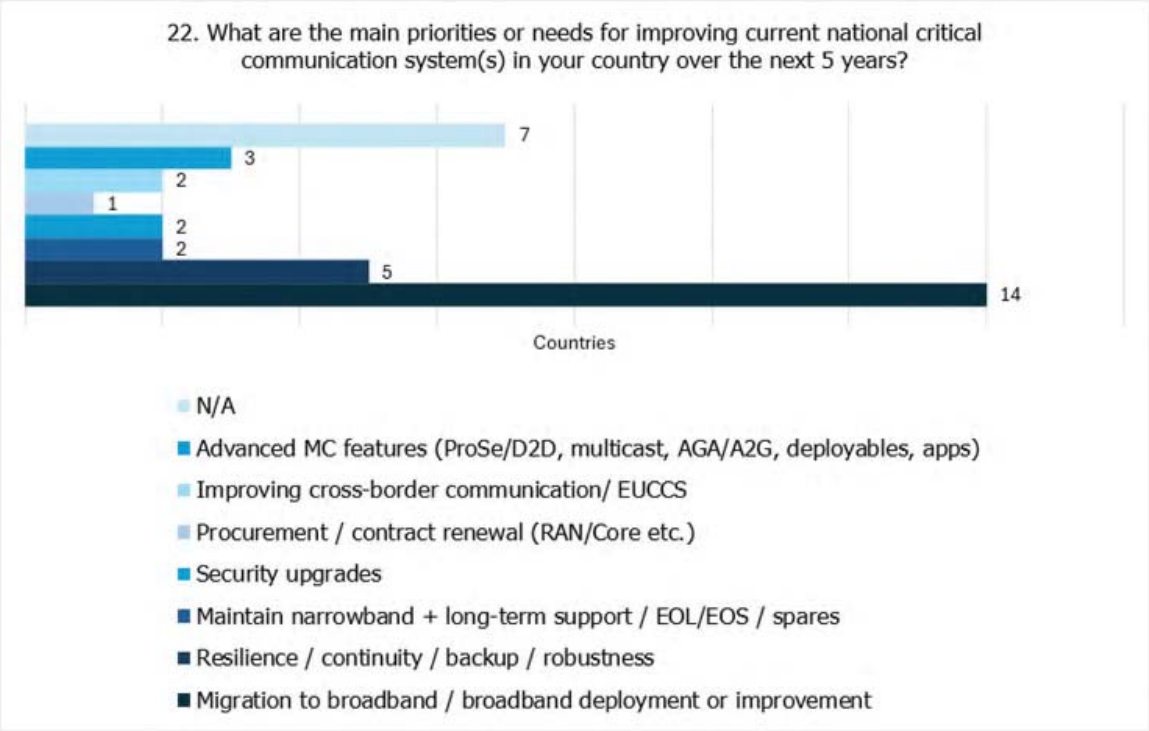


Figure 14. Reported plans or projects to update or upgrade national legacy narrowband systems



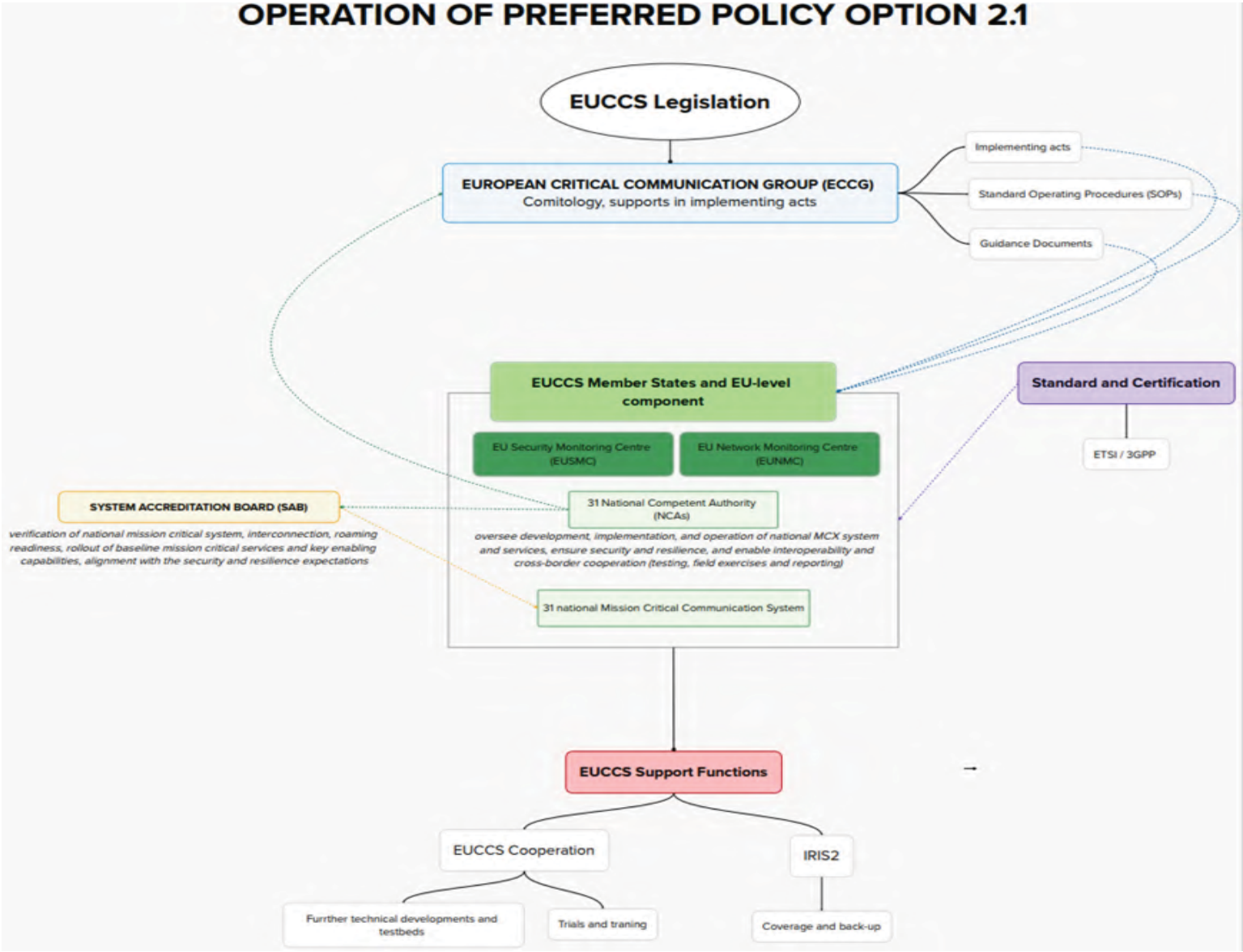
www.parlament.gv.at

Figure 15. Reported priorities or needs for improving current national CCS over the next 5 years



www.parlament.gv.at

Figure 16. Visualisation of operations of preferred policy option 2.1



www.parlament.gv.at

www.parlament.gv.at

Detailed overview of costs for Policy Options

7.2. POLICY OPTION 0 = Status quo

Cluster	Average one-off cost (CapEx)	Average annual recurrent cost (OpEx)	Average discounted OpEx over 7 years at 3% discount factor	Total average cost [1] = average CapEx + average discounted Opex
Cluster 1 – large countries (8: FR, RO, ES, SE, DE, IT, NO, PL)	€ 292,905,000.00	€ 67,481,250.00	€ 420,427,281.67	**€ 713,332,281.67**
Cluster 2 – medium countries (14: BE, CZ, DK, FI, NL, AT, BG, GR, HU, IE, LT, PT, SK, CH + LI)	€ 122,024,499,89	€ 48,127,168.22	€ 299,845,875.26	**€ 421,870,375.70**
Cluster 3 – small countries (8: EE, LV, LU, SI, HR, CY, IS, MT)	€ 55,997,000.00	€ 12,162,500.00	€ 75,775,816.44	**€ 131,772,816.44**
Total cost PO0 – Status quo: Sum of average costs (CapEx and OpEx over 7 years) for cluster 1 x 8 large Member States, cluster 2 x 12 medium Member States and cluster 3 x 8 small Member States = € 713,332,281.67 x 8 + € 421,870,375.70 x 14 + € 131,772,816.44 x 8				**€ 12,667,026,044.72**

7.3 POLICY OPTION 1 = Voluntary interconnectivity with other Member States

Costs for Member States				
Cost items	**Average one-off cost (CapEx) per EU MS and SAC**	**Average annual recurrent cost (OpEx) per EU MS and SAC**	**Discounted average OpEx over 7 years at 3% discount factor**	**Total average cost = average CapEx + average discounted OpEx**
Adjustment costs				
Cost of setting up and maintaining 1 bilateral connection	€ 1,400,041.00	€ 190,559.20	€ 1,187,237.74	€ 2,587,278.74
Additional human resources for 1 bilateral connection	€ 48,702.00	€ 39,736.03	€ 247,566.73	€ 296,268.73
Other adjustment costs	*Insufficient data*	*Insufficient data*	*Insufficient data*	*Insufficient data*
Administrative costs				
Organisation of trainings for 1 bilateral connection	€ 394,608.00	€ 85,123.24	€ 530,341.86	€ 924,949.86
Other administrative costs for 1 bilateral connection	€ 65,727.00	€ 32,343.67	€ 201,510.20	€ 267,237.20
Total	€ 1,351,428.20	€ 238,980.34	€ 1,488,915.14	**€ 2,840,343.34**
Costs for the European Union				
Cost items	**One-off cost (CapEx)**	**Annual recurrent cost (OpEx)**	**Discounted OpEx over 7 years at 3% discount factor**	**Total cost = CapEx + discounted OpEx**
Continuation of Mission Critical Communication Group mandate and management		€ 350,000.00	€ 2,180,599.03	€ 2,180,599.03
Guidance/ soft-law (incl. Standard Operating Procedures Handbook)	€ 167,070.00	€ 167,070.00	€ 1,040,893.37	€ 1,207,963.37
Total	€ 167,070.00	€ 517,070.00	€ 3,221,492.41	**€ 3,388,562.41**
Total cost PO1 – Voluntary interconnectivity: Total average cost for Member States for 1 bilateral interconnection x Median estimate of the # of interconnections + total costs for the EU = € 2,840,343.34 x 56 + € 3,388,562.41. Note that his estimate covers the costs only for those 11 Member States which replied that they are planning or willing to create interconnections with other Member States.				**€ 162,447,789.18**

www.parlament.gv.at

7.4 POLICY OPTION 2 = EU component interconnecting all Member States' national critical communication systems (system of systems) - Sub-option 1 – decentralised governance at EU level

Costs for Member States									
Cost items	**Average CapEx per Member State in cluster 1**	**Average annual OpEx per Member State in cluster 1**	**Discounted average OpEx over 7 years at 3% discount factor per cluster 1**	**Average CapEx per Member State in cluster 2**	**Average annual OpEx per Member State in cluster 2**	**Discounted average OpEx over 7 years at 3% discount factor per cluster 2**	**Average CapEx per Member State in cluster 3**	**Average annual OpEx per Member State in cluster 3**	**Discounted average OpEx over 7 years at 3% discount factor per cluster 3**
Adjustment costs									
Connection to the EUCCS: Network and infrastructure	€ 30,433,333.33	€ 4,250,000.00	€ 26,478,702.56	€ 392,581.33	€ 96,290.67	€ 599,918.10	€ 2,738,050.00	€ 710,350.00	€ 4,425,681.50
Connection to the EUCCS: User equipment and applications	€ 7,500,000.00	€ 2,456,886.67	€ 15,307,099.12	€ 23,158,891.02	€ 11,630,109.22	€ 72,458,871.26	€ 5,768,516.67	€ 1,345,061.11	€ 8,380,111.31
Connection to the EUCCS: Software licences and maintenance	€ 9,500,000.00	€ 670,000.00	€ 4,174,289.58	€ 9,083,473.83	€ 3,977,744.25	€ 24,782,472.19	€ 927,812.50	€ 155,937.50	€ 971,534.75
Set-up of a national single point of contact	€ 611,198.00	€ 275,000.00	€ 1,713,327.81	€ 45,088.00	€ 40,088.00	€ 249,759.58	€ 231,484.50	€ 109,279.50	€ 680,842.21
Critical communication support services	€ 611,198.00	€ 328,443.33	€ 2,046,294.90	€ 54,436.00	€ 77,218.00	€ 481,089.99	€ 135,887.50	€ 141,308.33	€ 880,390.90

www.parlament.gv.at

Additional human resources	€ 600,796.00	€ 625,804.00	€ 3,898,935.99	€ 51,022.00	€ 46,022.00	€ 286,730.08	€ 155,940.00	€ 140,868.89	€ 877,653.04
Other adjustment costs (ex. SOC)	*Insufficient data*	*Insufficient data*	*Insufficient data*	€ 7,345,850.07	€ 1,014,016.06	€ 6,317,607.00	€ 127,783.33	€ 203,705.56	€ 1,269,143.25
Administrative costs									
Reporting tools for the national competent authority	€ 750,000.00	€ 63,333.33	€ 394,584.59	€ 280,357.13	€ 37,142.86	€ 231,410.51	€ 215,237.50	€ 53,412.50	€ 332,774.99
Additional human resources in charge of reporting and statistical work	€ 483,406.00	€ 174,241.33	€ 1,085,572.81	€ 37,588.00	€ 36,338.00	€ 226,396.02	€ 106,939.50	€ 73,597.83	€ 458,535.33
Organisation of trainings	€ 891,320.00	€ 127,465.33	€ 794,145.09	€ 12,345,739.99	€ 32,262.00	€ 201,001.39	€ 118,350.00	€ 54,616.67	€ 340,277.29
Other administrative costs	*Insufficient data*	*Insufficient data*	*Insufficient data*	€ 83,266.67	€ 83,266.67	€ 518,774.89	€ 83,383.33	€ 66,691.67	€ 415,507.95
Total	€ 33,298,959.00	€ 7,722,130.50	€ 48,111,058.03	€ 38,923,190.16	€ 11,684,407.29	€ 72,797,163.60	€ 9,007,535.25	€ 2,563,747.75	€ 15,972,873.91

Cluster	Average one-off cost (CapEx)	Average annual recurrent cost (OpEx)	Average discounted OpEx over 7 years at 3% discount factor	Total average cost [2] = average CapEx + average discounted Opex
Cluster 1 – large countries (8: FR, RO, ES, SE, DE, IT, NO, PL)	€ 33,298,959.00	€ 7,722,130.50	€ 48,111,058.03	**€ 81,410,017.03**
Cluster 2 – medium countries (14: BE, CZ, DK, FI, NL, AT, BG, GR, HU, IE, LT, PT, SK, CH + LI)	€ 38,923,190.16	€ 11,684,407.29	€ 72,797,163.60	**€ 111,720,353.76**
Cluster 3 – small countries (8: EE, LV, LU, SI, HR, CY, IS, MT)	€ 9,007,535.25	€ 2,563,747.75	€ 15,972,873.91	**€ 24,980,409.16**
Total Member States cost: Total average cost cluster 1 x 8 of Member States in cluster 1 + Total average cost cluster 2 x 14 Member States cluster 2 + Total average cost cluster 3 x 8 Member States in cluster 3 = € 81,410,017.03 x 8 + € 111,720,353.76 x 14 + € 24,980,409.16 x 8.				**€ 2,415,208,362.20**

www.parlament.gv.at

Costs for the European Union				
Cost items	**One-off cost (CapEx)**	**Annual recurrent cost (OpEx)**	**Discounted OpEx over 7 years at 3% discount factor**	**Total cost = CapEx + discounted OpEx**
Adjustment costs				
Dedicated IPX network	€ -	€ 10,000,000.00	€ 62,302,829.55	€ 62,302,829.55
Standardisation and certification	€ -	€ 1,500,000.00	€ 9,345,424.43	€ 9,345,424.43
Satellite connectivity	€ 100,000,000.00	€ 20,000,000.00	€ 124,605,659.10	€ 224,605,659.10
Testbeds	€ -	€ 50,000,000.00	€ 311,514,147.76	€ 311,514,147.76
European Security Monitoring Centre	€ -	€ 10,000,000.00	€ 62,302,829.55	€ 62,302,829.55
European Network Monitoring Centre	€ -	€ 10,000,000.00	€ 62,302,829.55	€ 62,302,829.55
European Critical Communications Group Committee	€ -	€ 1,000,000.00	€ 6,230,282.96	€ 6,230,282.96
System Accreditation Board	€ -	€ 5,000,000.00	€ 31,151,414.78	€ 31,151,414.78
EUCCS Cooperation	€ 1,000,000.00	€ 50,000,000.00	€ 311,514,147.76	€ 312,514,147.76
Guidance/soft-law (Standard Operating Procedures Handbook)	€ 167,070.00	€ 167,070.00	€ 1,040,893.37	€ 1,207,963.37
Administrative costs				
Additional human resources	€ -	€ 1,670,700.00	€ 10,408,933.73	€ 10,408,933.73
Costs for training staff	€ -	€ 10,000,000.00	€ 62,302,829.55	€ 62,302,829.55
Total	€ 101,167,070.00	€ 169,337,770.00	€ 1,055,022,222.11	**€ 1,156,189,292.11**

Total cost PO2.1– System of systems with decentralised governance (Total average cost cluster 1 x 8 Member States in cluster 1 + Total average cost cluster 2 x 14 Member States in cluster 2 + Total average cost cluster 3 x 8 Member States in cluster 3) + Total costs for the EU = (€ 81,410,017.03 x 8 + € 111,720,353.76 x 14 + € 24,980,409.16 x 8) = € 2,415,208,362.20 + € 1,156,189,292.11	**€ 3,571,397,654.31**

www.parlament.gv.at

7.5 POLICY OPTION 2 = EU component interconnecting all Member States' national critical communication systems (system of systems) - Sub-option 2 – centralised governance at EU level

Costs for Member States									
Cost items	**Average CapEx per Member State in cluster 1**	**Average annual OpEx per EU MS and SAC in cluster 1**	**Discounted average OpEx over 7 years at 3% discount factor per cluster 1**	**Average CapEx per EU MS and SAC in cluster 2**	**Average annual OpEx per EU MS and SAC in cluster 2**	**Discounted average OpEx over 7 years at 3% discount factor per cluster 2**	**Average CapEx per EU MS and SAC in cluster 3**	**Average annual OpEx per EU MS and SAC in cluster 3**	**Discounted average OpEx over 7 years at 3% discount factor per cluster 3**
Adjustment costs									
Connection to the EUCCS: Network and infrastructure	€ 30,433,333.33	€ 4,250,000.00	€ 26,478,702.56	€ 392,581.33	€ 96,290.67	€ 599,918.10	€ 2,738,050.00	€ 710,350.00	€ 4,425,681.50
Connection to the EUCCS: User equipment and applications	€ 7,500,000.00	€ 2,456,886.67	€ 15,307,099.12	€ 23,158,891.02	€ 11,630,109.22	€ 72,458,871.26	€ 5,768,516.67	€ 1,345,061.11	€ 8,380,111.31
Connection to the EUCCS: Software licences and maintenance	€ 9,500,000.00	€ 670,000.00	€ 4,174,289.58	€ 9,083,473.83	€ 3,977,744.25	€ 24,782,472.19	€ 927,812.50	€ 155,937.50	€ 971,534.75
Set-up of a national single point of contact	€ 611,198.00	€ 275,000.00	€ 1,713,327.81	€ 45,088.00	€ 40,088.00	€ 249,759.58	€ 231,484.50	€ 109,279.50	€ 680,842.21
Critical communication support services	€ 611,198.00	€ 328,443.33	€ 2,046,294.90	€ 54,436.00	€ 77,218.00	€ 481,089.99	€ 135,887.50	€ 141,308.33	€ 880,390.90
Additional human resources	€ 600,796.00	€ 625,804.00	€ 3,898,935.99	€ 51,022.00	€ 46,022.00	€ 286,730.08	€ 155,940.00	€ 140,868.89	€ 877,653.04
Other adjustment costs (ex. SOC)	*Insufficient data*	*Insufficient data*	*Insufficient data*	€ 7,345,850.07	€ 1,014,016.06	€ 6,317,607.00	€ 127,783.33	€ 203,705.56	€ 1,269,143.25

www.parlament.gv.at

Administrative costs									
Reporting tools for the national competent authority	€ 750,000.00	€ 63,333.33	€ 394,584.59	€ 280,357.13	€ 37,142.86	€ 231,410.51	€ 215,237.50	€ 53,412.50	€ 332,774.99
Additional human resources in charge of reporting and statistical work	€ 483,406.00	€ 174,241.33	€ 1,085,572.81	€ 37,588.00	€ 36,338.00	€ 226,396.02	€ 106,939.50	€ 73,597.83	€ 458,535.33
Organisation of trainings	€ 891,320.00	€ 127,465.33	€ 794,145.09	€ 12,345,739.99	€ 32,262.00	€ 201,001.39	€ 118,350.00	€ 54,616.67	€ 340,277.29
Other administrative costs	*Insufficient data*	*Insufficient data*	*Insufficient data*	€ 83,266.67	€ 83,266.67	€ 518,774.89	€ 83,383.33	€ 66,691.67	€ 415,507.95
Total	€ 33,298,959.00	€ 7,722,130.50	€ 48,111,058.03	€ 38,923,190.16	€ 11,684,407.29	€ 72,797,163.60	€ 9,007,535.25	€ 2,563,747.75	€ 15,972,873.91

Cluster	Average one-off cost (CapEx)	Average annual recurrent cost (OpEx)	Average discounted OpEx over 7 years at 3% discount factor	Total average cost [3] = average CapEx + average discounted Opex
Cluster 1 – large countries (8: FR, RO, ES, SE, DE, IT, NO, PL)	€ 33,298,959.00	€ 7,722,130.50	€ 48,111,058.03	**€ 81,410,017.03**
Cluster 2 – medium countries (14: BE, CZ, DK, FI, NL, AT, BG, GR, HU, IE, LT, PT, SK, CH + LI)	€ 38,923,190.16	€ 11,684,407.29	€ 72,797,163.60	**€ 111,720,353.76**
Cluster 3 – small countries (8: EE, LV, LU, SI, HR, CY, IS, MT)	€ 9,007,535.25	€ 2,563,747.75	€ 15,972,873.91	**€ 24,980,409.16**
Total Member States' cost: Total average cost cluster 1 x 8 Member States in cluster 1 + Total average cost cluster 2 x 14 Member States in cluster 2 + Total average cost cluster 3 x 8 Member States in cluster 3 = € 81,410,017.03 x 8 + € 111,720,353.76 x 14 + € 24,980,409.16 x 8				**€ 2,415,208,362.20**

www.parlament.gv.at

Costs for the European Union				
Cost items	**One-off cost (CapEx)**	**Annual recurrent cost (OpEx)**	**Discounted OpEx over 7 years at 3% discount factor**	**Total cost = CapEx + discounted OpEx**
Adjustment costs				
Dedicated IPX network	€ -	€ 10,000,000.00	€ 62,302,829.55	€ 62,302,829.55
Standardisation and certification	€ -	€ 1,500,000.00	€ 9,345,424.43	€ 9,345,424.43
Satellite connectivity	€ 100,000,000.00	€ 20,000,000.00	€ 124,605,659.10	€ 224,605,659.10
Testbeds	€ -	€ 50,000,000.00	€ 311,514,147.76	€ 311,514,147.76
EU competent authority	€ 1,000,000.00	€ 75,000,000.00	€ 467,271,221.64	€ 468,271,221.64
European Critical Communications Group Committee	€ -	€ 1,000,000.00	€ 6,230,282.96	€ 6,230,282.96
Guidance/soft-law (Standard Operating Procedures Handbook)	€ 167,070.00	€ 167,070.00	€ 1,040,893.37	€ 1,207,963.37
Administrative costs				
Additional human resources	€ -	€ 1,253,025.00	€ 7,806,700.30	€ 7,806,700.30
Costs for training staff	€ -	€ 10,000,000.00	€ 62,302,829.55	€ 62,302,829.55
Total	€ 101,167,070.00	€ 168,920,095.00	€ 1,052,419,988.67	**€ 1,153,587,058.67**
Total cost PO2.2 – System of systems with centralised governance (Total average cost cluster 1 x 8 Member States in cluster 1 + Total average cost cluster 2 x 14 Member States in cluster 2 + Total average cost cluster 3 x 8 Member States in cluster 3) + Total costs for the EU = (€ 81,410,017.03 x 8 + € 111,720,353.76 x 14 + € 24,980,409.16 x 8) = € 2,415,208,362.20 + € 1,153,587,058.67				**€ 3,568,795,420.87**

[1] Cluster averages are calculated of basis of data gathered from the underlined Member States in each cluster. In total 30 and not 31 EU Member States and Schengen-associate countries have been calculated, as CH and LI have been counted once, as they will share one system.

www.parlament.gv.at

7.6 Current and planned arrangements of selected Member States with mobile network operators

In **France**, the planned arrangement for the national broadband critical communications system relies on commercial mobile network operators as connectivity providers under a contractual framework defined for the Radio du Futur (RRF) programme. The model is not based on a fully dedicated nationwide mobile network operated exclusively for first responders, but on the use of commercial mobile infrastructure with specific service requirements for critical users, including quality of service, priority and pre-emption mechanisms, resilience commitments, and security constraints. A commercial framework is established with two mobile network operators providing full quality of service, priority and pre-emption capabilities, while national roaming agreements are in place with two additional operators, offering extended coverage on a best-effort quality of service basis, with fair compensation defined in accordance with the French regulatory framework. The costs related to mobile network operators are covered through the overall contracts concluded with the operators, amounting to € 150 million (excluding VAT) over a four-year period, as defined in the public procurement process. This includes access to mobile connectivity, implementation and activation of priority and quality of service mechanisms, testing, integration, operational support, and resilience-related commitments. Traffic prioritisation is not identified as a major recurring cost driver, but rather as one component of a broader service package negotiated contractually with the operators.

Finland signed the contract for € 48 million (excluding VAT) with its primary mobile network operator in May 2020 for a 10 year's period. The integration, testing and acceptance for data services was finished in February 2022. In parallel, the processes were developed to maintain interoperability of mission-critical services with the existing TETRA system, thereby smoothening the migration to broadband. The monthly fee for end-users is € 60, covering the terminal, voice, video and data.

In **Norway**, the Norwegian Communications Authority (Nkom), is going to collaborate with the three national mobile network operators to facilitate the use of mobile networks as carriers of broadband critical communication services. Preparations are in a pre-project phase, with requests made for government funding. Three parallel agreements for the delivery of a radio access and core network in the form of dedicated 5G slices are envisaged. The supply of the mission-critical services platform and of mobile devices will be subject to separate public procurements. At this stage, no cost estimates can be shared.

Belgium plans to rely on a primary mobile network operator for the radio access network services of its future broadband critical communications system. These services — including mission-critical services, voice telephony and internet connectivity — are being procured through a public procurement procedure open to the four Belgian mobile network operators, one of which will become the primary mobile network operator. Video is expected to be one of the most demanding applications in terms of future data usage, although it is still only used to a limited extent by first responders today. Belgium is separating the procurement of the dedicated core, for which the supplier does not necessarily need to be a Belgian mobile network operator, and the procurement of the radio access network services. If a Belgian mobile network operator is involved in the core procurement, strict separation arrangements must apply. As the procurement procedures are still ongoing, no cost figures related to mobile network operators can yet be shared. The relevant costs will be covered through the overall contracts resulting from these procurement procedures.

7.7 Methodology for the cost assessment

The methodology applied for the cost estimates is the same used for the study provided by the external contractor.

The cost assessment measured incremental costs against the baseline scenario, that is, the additional costs arising under each policy option relative to continuation of the status quo. The analysis distinguished between adjustment costs and administrative costs, with costs separated into one-off (CapEx) and recurrent components (OpEx). A 7-year time horizon was chosen to mirror the phased roll-out of the EUCCS delineated in the Operational Plan, which foresees implementation milestones in 2030, 2033 and 2036. Recurrent costs were then expressed in present-value terms using a 3% social discount factor in real terms. Nothing indicates that the initiative would increase the costs of the Member States in terms of the Cost data for EU-level public authorities were estimated based on working meetings conducted with the European Commission and technical experts. The absence of incremental costs for businesses and other economic operators has been confirmed through targeted interviews as well as working meetings with the European Commission and relevant business associations and industry representatives.

Given the limited availability of sufficiently complete cost data from the targeted survey for EU Member States (as many Member States have not started yet with preparing for or are in early stages of their transition to broadband), a shortlist of 13 more advanced countries (France, Romania, Spain, Sweden, Belgium, Czech Republic, Denmark, Finland, the Netherlands, Estonia, Latvia, Luxembourg, Slovenia) was established to provide the main evidence base for the public authorities' cost assessment. The actual entries reflect a combination of survey responses and additional evidence collected through targeted cost interviews with shortlisted country representatives. For two Member States which provided far below average cost estimates (Netherlands, Finland), the Commission asked those Member States for check once again their cost estimates which were then corrected, matching more closely the other cost estimates.

The costs of the status quo (PO0) comprise only the Member States' public authorities' related costs, given that under this policy option, there is no EU-level intervention.

Since only 13 Member States were able to provide complete country-specific cost data, the cost estimation was based on extrapolation by country cluster. Member States were grouped into three system-size clusters — (1) large, (2) medium and (3) small — using three dimensions: (i) population ([101]), (ii) total land area in km² ([102]), and, where available, (iii) the number of national critical communications end-users ([103]). Applying a dominance rule, countries were classified as large where they were deemed large on any available dimension, as small where they were deemed small on all available dimensions, and

(101) Eurostat, *Population on 1 January (tps00001)* (2025). https://ec.europa.eu/eurostat/databrowser/view/tps00001/default/map?lang=en.
(102) For EU MS: Eurostat, *Land cover overview by NUTS 2 region (lan_lcv_ovw)* (2025). https://ec.europa.eu/eurostat/databrowser/view/lan_lcv_ovw/default/table?lang=en accessed 10 March 2026; For SAC: World Bank Group, *Land area (sq. km) (AG.LND.TOTL.K2)* (2024). https://data.worldbank.org/indicator/AG.LND.TOTL.K2.
(103) Data extracted from publicly available information or collected during the Study.

www.parlament.gv.at

otherwise as medium. For countries without complete cost data, cost inputs were then proxied by the average values observed for comparable Member States within the same cluster ([104]). The resulting distribution comprised 8 countries in cluster 1 (FR, DE, IT, NO, PL, RO, ES, SE), 14 in cluster 2 (AT, BE, BG, CZ, DK, FI, GR, HU, IE, LT, NL, PT, SK, CH + LI) and 8 in cluster 3 (HR, CY, EE, IS, LV, LU, MT, SI).

The calculation of costs under PO0 was therefore based on the average cost per country within each cluster, split between CapEx and annual OpEx for three cost items: interconnection of domestic critical communication systems, transition to broadband, and related adaptation costs. Annual recurrent costs were converted into present-value terms over the 7-year assessment period using a 3% real discount rate. For each cluster c, the total cost was calculated as:

$$\text{Total cost}_c = n_c \times \left[\text{CapEx}_c + \sum_{t=1}^{7} \frac{\text{OpEx}_c}{(1+r)^t}\right]$$

where n_c is the number of countries in a given cluster c, $\text{CapEx}_c$is the average one-off investment cost per country in that cluster, $\text{OpEx}_c$is the average annual recurrent cost per country in that cluster, and r is the real discount rate. The total PO0 cost was then calculated by summing the three cluster totals:

$$\text{Total PO0 cost} = \text{Total cost}_{c1} + \text{Total cost}_{c2} + \text{Total cost}_{c3}$$

For the voluntary technical interconnection option (PO1), the cost assessment did not assume full interconnection across all Member States but covered only those 11 countries that expressed a willingness to establish interconnections and on the number of interconnections they indicated. The average unit cost per bilateral interconnection was used as the other core metric for estimating PO1 costs, and the same cost figure was applied across all Member States. This assumes that, while actual national costs may vary depending on system configuration and implementation choices, the average cost observed in the available evidence provides a reasonable basis The total cost for Member States' public authorities of PO1 was therefore calculated as:

$$\text{Total PO1 cost for Member States' public authorities} = N \times \left[CapEx_{unit} + \sum_{t=1}^{7} \frac{OpEx_{unit}}{(1+r)^t}\right]$$

where N is the expected number of new bilateral interconnections, $CapEx_{unit}$is the average one-off investment cost per bilateral interconnection, $OpEx_{unit}$is the average annual recurrent cost per bilateral interconnection, and r is the real discount rate.
PO1 also entailed EU-level costs linked to the continuation of the MCCG mandate and the preparation of guidance and other soft-law instruments, including the EUCCS Handbook (standard operating procedures).

(104) This approach was validated in a dedicated working meeting on costs with the European Commission and technical experts, organised on 04 March 2026.

www.parlament.gv.at

For the system of systems policy options (PO2), the cost assessment assumed full participation by all Member States, as interconnection through the EU component of the EUCCS and interoperability of national critical communication systems would be mandatory under an EU legislative act. The assessment, therefore, covered 30 implementation cases, with Switzerland and Liechtenstein treated jointly as one case.

As for PO0, given that not all Member States were able to provide complete country-specific cost data for PO2, the cost estimation was based on extrapolation by country cluster, grouping Member States into three system-size clusters as above.

The calculation of Member States' public authorities' costs under PO2 was therefore based on the average cost per country within each cluster, split between CapEx and annual OpEx. Annual recurrent costs were converted into present-value terms over the 7-year assessment period using a 3% real discount rate. For each cluster c, the total cost was calculated as:

$$\text{Total cost}_c = n_c \times \left[\text{CapEx}_c + \sum_{t=1}^{7} \frac{\text{OpEx}_c}{(1+r)^t}\right]$$

where n_c is the number of countries in a given cluster c, $\text{CapEx}_c$is the average one-off investment cost per country in that cluster, $\text{OpEx}_c$is the average annual recurrent cost per country in that cluster, and r is the real discount rate. The total PO2 cost for Member States' public authorities was then calculated by summing the three cluster totals:

$$\text{Total PO2 cost for Member States public authorities} = \text{Total cost}_{c1} + \text{Total cost}_{c2} + \text{Total cost}_{c3}$$

EU-level costs linked to the establishment, governance and operation of the EU component of the EUCCS. These costs were estimated separately for the two governance sub-options considered: 2.1 – decentralised EU governance, and 2.2 – EU competent authority. For each sub-option, and as for PO1, the total EU-level costs were calculated as the sum of one-off costs and discounted recurrent annual costs over the 7-year assessment period:

$$\text{Total PO2 cost for EU-level public authorities} = \text{CapEx}_{EU} + \sum_{t=1}^{7} \frac{\text{OpEx}_{EU}}{(1+r)^t}$$

where CapEx_{EU}represents the one-off EU-level investment costs and OpEx_{EU} the annual recurrent EU-level costs.
The **overall total PO2 cost** was obtained by adding Member States' costs and the EU-level costs:

$$\text{Total PO2 cost} = \text{Total PO2 cost for Member States' public authorities} + \text{Total PO2 cost for EU-level public authorities}$$

www.parlament.gv.at

Annex 7.8 Economic impact on Mobile Network Operators (MNOs)

The information provided in the draft impact assessment on the obligations for MNOs is provided via dedicated interviews with technical experts from Finland, Belgium, Norway and France. Those Member States have contractual arrangements with Mobile Network Operators to facilitate mission-critical communication.

www.parlament.gv.at

The synthesis of the information collected indicates that EUCCS is not expected to new infrastructure costs for mobile network operators, as the required functionalities are, in most cases, already embedded in commercial 4G/5G standards and infrastructures. The main economic impact relates instead to contractual service levels, resilience requirements, operational integration, and governance arrangements defined at national level.

The EUCCS does not add costs for MNOs in terms of traffic because:

- emergency services users typically represent less than 1% of total subscribers;
- prioritisation mechanisms are activated dynamically only during congestion situations;
- these situations remain infrequent and temporary;
- operators already manage comparable priority mechanisms today, including emergency call handling and network management policies.

Therefore, traffic prioritisation itself is not considered a standalone cost driver. Quality of service, priority and pre-emption mechanisms are standardised native features of 4G and 5G networks defined by 3GPP and largely already implemented by operators. Mission-critical broadband bearers, such as quality-of-service class identifiers for prioritising data traffic, are basic services of radio access network vendors and no extra costs occur, or licences are needed.
No large-scale additional radio network deployment is expected for EUCCS which is designed to leverage on existing 4G/5G infrastructures. Consequently, incremental CapEx for MNOs is expected to remain limited and mainly relates to:

- configuration and activation of existing 3GPP mission-critical capabilities;
- adaptation of operational support systems;
- possible resilience enhancements required contractually by Member States;
- testing, validation and interoperability activities.

The main recurring costs therefore fall under OpEx and relate to:

- operational support;
- maintenance of prioritisation and quality of service configurations;
- resilience commitments;
- service assurance;
- interoperability management;
- operational coordination with public authorities;
- testing and lifecycle management.

It is indeed left to the contractual agreements between Member States and the Mobile Network Operators of whom they are customers to agree on compensation, or rather subscription fees for the mission critical services. Compensation mechanisms primarily cover:

- contractual service obligations;
- resilience and availability guarantees;

www.parlament.gv.at

- operational support requirements;
- testing and interoperability obligations;
- security requirements;
- and potentially dedicated operational arrangements.

This goes beyond compensating MNOs for the mere activation of prioritisation features.

The MNOs themselves were consulted on this issue to verify if they would expect additional cost or burden. Given that no MNO replied to the initial industry survey conducted as part of the supporting study, a dedicated in-person consultation for three major industry organisations was organised. Participants from the GSM Association (GSMA) representing the MNOs, as well as the Critical Communication Association and Public Safety Communication Europe were consulted and invited as a follow-up to also submit any concerns vie the Commission Open Public Consultation. Only one individual MNO (Telefonica) replied to the OPC without raising fundamental concerns against the concept of obligations for MNOs on critical communication, as long as those were proportionate and limited to what was necessary.

www.parlament.gv.at

7.9 Key performance indicators for monitoring and evaluation

Specific Objectives	Policy Measure	Indicator	Definition / Measurement	Collection Method	Responsible entity	Recommended frequency	Priority
Objective 1	**PM2.1**: Establishment of governance structures at the national and EU levels, as well as of a European Critical Communications Group Committee	Designate the national competent authority per EU Member States and define its role and responsibilities	Confirm that a National Competent Authority has been designated per EU Member States and its role and responsibilities are defined through a notification to the European Commission	Notification to the EC by EU Member States	EU Member States National Competent Authorities	Once	High
		Designate the competent EU body and define role and responsibilities	Confirm that a competent authority has been designated at EU level and its role and responsibilities are defined	Published EU legal act	European Commission	Once	High
		Establish the European Critical Communications Group Committee and define its role and responsibilities	Confirm the establishment of the European Critical Communications Group Committee replacing the current Mission Critical Communication Group	Published EU legal act	European Commission	Once	High
Objective 2	**PM2.2**: EU-level monitoring of compliance and maturity assessment *via* a System Accreditation Board	Publish a report on the compliance and maturity assessment of national critical communication systems with the requirements of the EU legal act	Report on the EU Member States alignment with EUCCS security and resilience practices and progressive uptake of broadband solutions and European	Reporting received by System Accreditation Board from EU Member States National	System Accreditation Board	Annually	High

www.parlament.gv.at

Specific Objectives	Policy Measure	Indicator	Definition / Measurement	Collection Method	Responsible entity	Recommended frequency	Priority
			Telecommunications Standards Institute/Global Certification Forum standardisation and certifications as these mature	Competent Authorities			
		Establish a System Accreditation Board to oversee national critical communication systems readiness to connect to the EUCCS	Confirm the establishment of the System Accreditation Board	Published EU legal act	European Commission	Once	High
Objective 1	**PM2.3**: Reporting obligations for EU Member States, as well as operators of critical communication systems and the creation of the European Critical Communication System Security Monitoring Centre	Interconnection of each Member States national critical communication systems (e.g. police, ambulance, and fire brigade)	Number of EU Member States connected to the EUCCS	Reporting by EU Member States National Competent Authorities	European Critical Communication System Security Monitoring Centre	Annually	High
		Interconnection of emergency services	Number of emergency services with connectivity to the EUCCS	Reporting by EU Member States National Competent Authorities	European Critical Communication System Security Monitoring Centre	Annually	High
		Interconnection of Public Protection and Disaster	Number of Public Protection and Disaster Relief	Reporting by EU Member States National	European Critical Communication System Security	Annually	High

www.parlament.gv.at

Specific Objectives	Policy Measure	Indicator	Definition / Measurement	Collection Method	Responsible entity	Recommended frequency	Priority
		Relief services across the EU and Schengen area	authorities connected to the EUCCS	Competent Authorities	Monitoring Centre		
		Increased cross-border operational mobility	Number of Public Protection and Disaster Relief roaming minutes on the EUCCS	Reporting by EU Member States National Competent Authorities	European Critical Communication System Security Monitoring Centre	Annually	High
		Volume of data traffic	Volume of communications (data) exchanged across IPX for EUCCS	Reporting by EU Member States National Competent Authorities	European Critical Communication System Security Monitoring Centre	Annually	Medium
		Establish the EUCCS Security Monitoring Centre	Confirm the establishment of the European Critical Communication System Security Monitoring Centre	Published EU legal act	European Commission	Once	High
Objective 3	**PM2.4**: Minimum requirements for national critical communication systems	EUCCS mission critical services interconnection setup time	Maximum 3 seconds connection time from control room authorisation for a Public Protection and Disaster Relief agent to be able to join a mission critical services group in a visited Member State	Reporting by EU Member States National Competent Authorities	European Critical Communication System Security Monitoring Centre	Annually	High

www.parlament.gv.at

Specific Objectives	Policy Measure	Indicator	Definition / Measurement	Collection Method	Responsible entity	Recommended frequency	Priority
		Seamless Public Protection and Disaster Relief 3GPP roaming	Public Protection and Disaster Relief users connect to visited critical communication systems networks in sub-second times.	Reporting by EU Member States National Competent Authorities	European Critical Communication System Security Monitoring Centre	Annually	High
		Compliance with NIS2 and EU Cybersecurity Act	Number of EU Member States critical communication systems complying with NIS2 and EU Cybersecurity Act standards	Reporting by EU Member States National Competent Authorities	European Critical Communication System Security Monitoring Centre	Annually	High
		Service quality	Percentage of Member States that have implemented the European Critical Communications Group recommended Quality of Service, Priority, and Pre-emption mechanisms and settings on their critical communication systems networks.	Reporting by EU Member States National Competent Authorities	European Critical Communication System Security Monitoring Centre	Annually	High
		Radio Access Network (RAN) resilience	Minimum 24-hour backup power capacity throughout the critical communication systems network.	Reporting by EU Member States National Competent Authorities	European Critical Communication System Security Monitoring Centre	Annually	High

www.parlament.gv.at

Specific Objectives	Policy Measure	Indicator	Definition / Measurement	Collection Method	Responsible entity	Recommended frequency	Priority
		Continuity and redundancy plans	Number of regular stress-testing and disaster recovery exercises.	Reporting by EU Member States National Competent Authorities	European Critical Communication System Security Monitoring Centre	Annually	High
Objective 3	**PM2.5:** Adherence to risk-based guidance on autonomy and sovereignty	Reduced dependency on third country suppliers	The extent to which EU Member States depend on high-risk third country suppliers.	Supplier registries	EU Member States	Annually	Medium
Objective 1	**PM2.6**: Establishment of the EU technical component(s) of the EUCCS	Successful completion of operational readiness testing and entry into operations of all central technical components as required by the European Critical Communications Group Committee (e.g. IPX, testbeds)	Successful operational readiness testing and entry into operations reports from authority(ies) responsible for central components.	Reported to the European Critical Communications Group Committee	Designated EU authority(ies)	Once	High
Objective 1	**PM2.7:** Establishment of the interconnection between national critical communication systems and the EUCCS	Successful completion of conformance testing of national critical communication systems against the EUCCS baseline and confirmation of operational readiness testing and entry into operations of national	Successful joint operational readiness testing and entry into operations reports from National Competent Authority and from central EU authority(ies)	Reported to the European Critical Communications Group Committee	Designated EU authority(ies) and Member States National Competent Authority	Once	High

www.parlament.gv.at

Specific Objectives	Policy Measure	Indicator	Definition / Measurement	Collection Method	Responsible entity	Recommended frequency	Priority
		critical communication systems connecting to EUCCS					
Objective 2	**PM2.8:** Obligations for Mobile Network Operators to support Public Protection and Disaster Relief requirements on national networks and while roaming	Roaming Service Quality	Percentage of Member States that have implemented the European Critical Communications Group recommended Quality of Service, Priority, and Pre-emption mechanisms and settings on their critical communication systems networks for roaming Public Protection and Disaster Relief agents from other Member States.	Reporting by EU Member States National Competent Authority	EUCCS Security Monitoring Centre	Annually	High
Objective 1	**PM2.9**: Standard Operating Procedures Handbook	Number of EU Member States complying with Standard Operating Procedures	Number of EU Member States that comply with Standard Operating Procedures in line with EUCCS minimum requirements as approved by the European Critical Communications Group, including evidence of implementation in practice (e.g. use in operations, alignment with EU-level	Reporting by Member States through standardised EU reporting template	EU Member States	Annual	High

www.parlament.gv.at

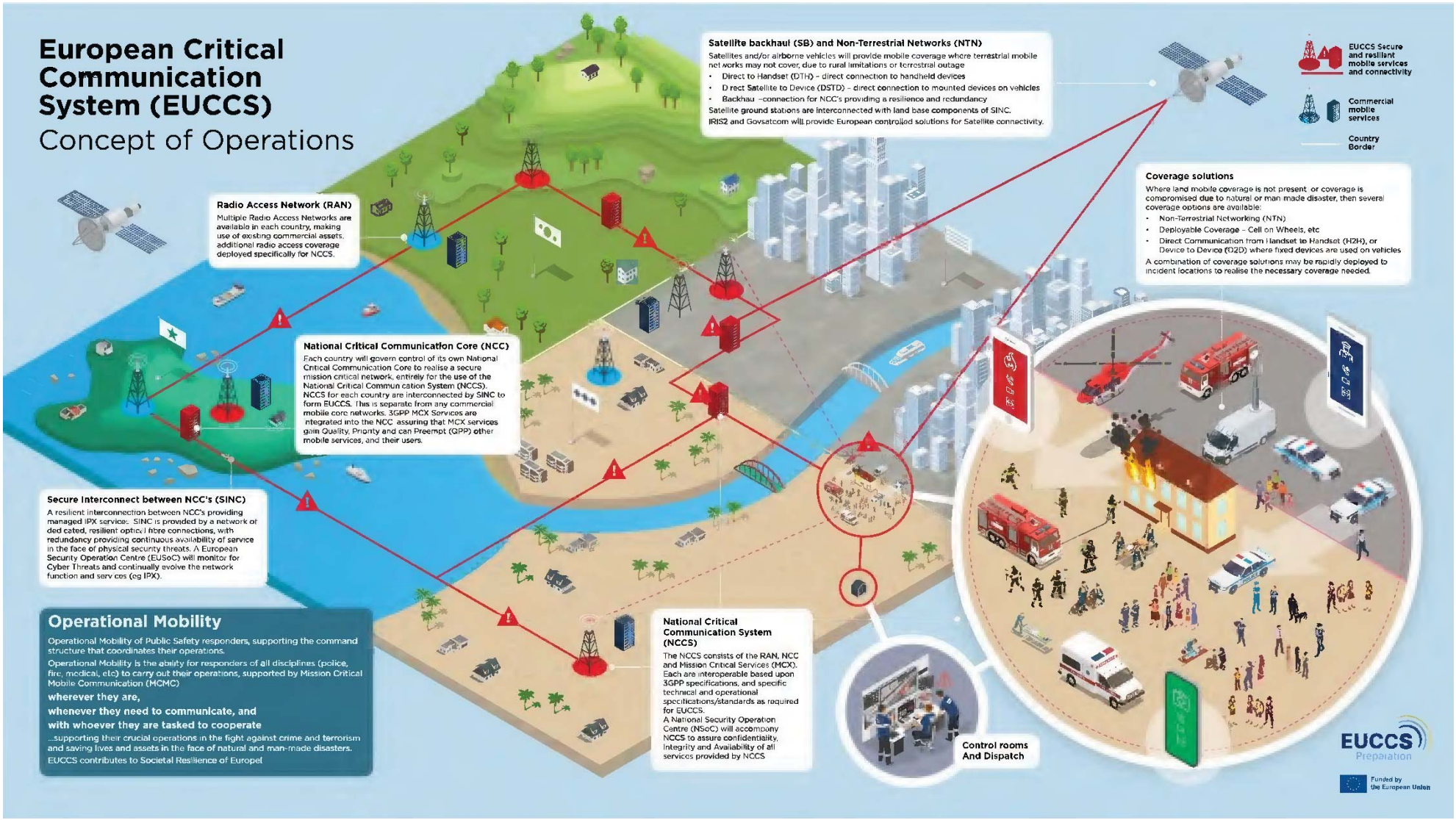
Specific Objectives	Policy Measure	Indicator	Definition / Measurement	Collection Method	Responsible entity	Recommended frequency	Priority
			Standard Operating Procedure baseline).				
		Annual review of the Standard Operating Procedures	Number of EU-level updates to the Standard Operating Procedure handbook, reflecting integration of operational lessons learned, technological developments, and evolving EUCCS requirements.	Documentation produced at EU level	European Critical Communications Group Committee	Annual	Medium
Objective 3	**PM2.10**: Requirement for national strategies or action plans for critical communications	Establishment of a national strategy or action plan for critical communications	Number of EU Member States with a national strategy or action plan for critical communications, in line with EUCCS minimum requirements.	Verification of an officially adopted strategy/action plan	EU Member States	Annual	High
		Progress on the implementation of the national strategy or action plan for critical communications	Annual report on the implementation of the strategy or action plan	Submission by Member States through standardised EU reporting template	EU Member States	Annual	Medium
Objective 1	**PM2.11**: Training, education and exercise programmes	Number of emergency services trained on use of the EUCCS for roaming	Total number of emergency services who have successfully completed EUCCS Standard Operating Procedures training	Attendance records and certification systems	• EU Member States National	Annual	High

www.parlament.gv.at

Specific Objectives	Policy Measure	Indicator	Definition / Measurement	Collection Method	Responsible entity	Recommended frequency	Priority
			programmes within a given reporting period.		Competent Authority • European Commission		
		Number of EUCCS joint exercises	Number of joint exercises conducted under the EUCCS framework within a given reporting period, involving two or more EU Member States, and testing critical communication capabilities.	EU-level coordination records	• EU Member States National Competent Authority • European Commission	Annual	High
		Number of emergency services participating in joint exercises	Total number of emergency services who participate in EUCCS joint exercises within a given reporting period.	Exercise attendance records	EU Member States / European Commission	Annual	High

www.parlament.gv.at

7.10 Visualisation of EUCCS Architecture



www.parlament.gv.at